(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平10－269289

(43)公開日　平成10年(1998)10月９日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　17/60		Ｇ０６Ｆ　15/21	３３０
1/00	３７０	1/00	３７０Ｆ
9/06	５５０	9/06	５５０Ｚ
15/00	３３０	15/00	３３０Ｚ
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｆ

審査請求　未請求　請求項の数37　ＯＬ　（全 39 頁）　最終頁に続く

(21)出願番号　特願平9－74182

(22)出願日　平成９年(1997)３月28日

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　真有　浩一
東京都品川区北品川６丁目７番35号　ソニー株式会社内

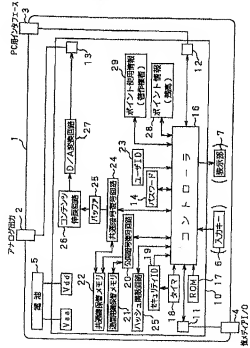
(74)代理人　弁理士　小池　晃　（外２名）

(54)【発明の名称】　ディジタルコンテンツ配付管理方法、ディジタルコンテンツ再生方法及び装置

(57)【要約】

【課題】　簡単に持ち運びができて何時でも何処でもディジタルコンテンツを楽しむことを可能とし、ディジタルコンテンツのコピー或いは不当な使用への防御として十分運用に耐え、且つ経済的なシステムを構築する。

【解決手段】　暗号化されたコンテンツ鍵を復号化し、セッション鍵を暗号化する公開暗号復号回路２０と、コンテンツ鍵やセッション鍵を保管する共通鍵保管メモリ２２と、公開暗号方式の鍵情報を保管する通信用鍵保管メモリ２１と、ポイント情報を格納するポイント情報格納メモリ２９と、ポイント使用情報を格納するポイント使用情報格納メモリ２８と、暗号化ディジタルコンテンツの復号化し、暗号化ポイント情報の復号化、ポイント使用情報の暗号化を行う共通暗号復号回路２４と、圧縮ディジタルコンテンツを伸長する伸長回路２６と、ディジタルコンテンツをＤ／Ａ変換するＤ／Ａ変換回路２７とを、１チップ化する。



【特許請求の範囲】

【請求項１】　ディジタルコンテンツを、当該ディジタルコンテンツ毎のコンテンツ鍵を用いて暗号化すると共に、圧縮するディジタルコンテンツ加工工程と、

上記加工したディジタルコンテンツを、通信相手側からのディジタルコンテンツ送信要求に応じて送信するコンテンツ送信工程と、

上記加工されたディジタルコンテンツの復号化に使用するコンテンツ鍵を暗号化し、通信相手側からのコンテンツ鍵送信要求に応じて送信するコンテン鍵送信工程と、

上記加工されたディジタルコンテンツを復号化する毎に減額される課金情報を暗号化し、通信相手側からの課金情報送信要求に応じて送信する課金情報送信工程と、

通信相手側から送信されてきた暗号化されたコンテンツ使用情報を受信して復号化するコンテンツ使用情報受信工程と、

上記コンテンツ使用情報に基づいて徴収した利用金を、上記ディジタルコンテンツの権利者に対して分配する利用金分配工程とを有してなることを特徴とするディジタルコンテンツ配付管理方法。

【請求項２】　上記コンテンツ鍵は共通鍵であることを特徴とする請求項１記載のディジタルコンテンツ配付管理方法。

【請求項３】　上記コンテンツ鍵を通信相手側の公開鍵を用いて暗号化することを特徴とする請求項１記載のディジタルコンテンツ配付管理方法。

【請求項４】　通信相手側から送信されてきた暗号化された共通鍵を受信して復号化する共通鍵復号化工程を有することを特徴とする請求項１記載のディジタルコンテンツ配付管理方法。

【請求項５】　上記共通鍵はセッション鍵であることを特徴とする請求項４記載のディジタルコンテンツ配付管理方法。

【請求項６】　上記課金情報送信工程では、課金情報を上記共通鍵を用いて暗号化することを特徴とする請求項４記載のディジタルコンテンツ配付管理方法。

【請求項７】　上記コンテンツ使用情報受信工程では、上記暗号化されたコンテンツ使用情報の復号化に上記共通鍵を用いることを特徴とする請求項４記載のディジタルコンテンツ配付管理方法。

【請求項８】　上記コンテンツ使用情報受信工程では、上記通信相手側からの上記課金情報の送信要求に伴って当該通信相手側から送信されてくる上記暗号化されたコンテンツ使用情報を受信することを特徴とする請求項１記載のディジタルコンテンツ配付管理方法。

【請求項９】　上記課金情報送信工程では、上記課金情報と共にコンテンツの使用条件を示す情報を送信することを特徴とする請求項１記載のディジタルコンテンツ配付管理方法。

【請求項１０】　暗号化及び圧縮処理によって加工されたディジタルコンテンツを受信して格納するコンテンツ受信工程と、

上記加工されたディジタルコンテンツの復号化に必要なコンテンツ鍵を要求するためのコンテンツ鍵要求情報を生成するコンテンツ鍵要求情報生成工程と、

上記コンテンツ鍵要求情報を暗号化して送信するコンテンツ鍵要求情報送信工程と、

上記コンテンツ鍵の要求に応じて送信されてきたコンテンツ鍵を受信するコンテンツ鍵受信工程と、

上記コンテンツ鍵に施されている暗号化を復号化するコンテンツ鍵復号化工程と、

上記暗号化されたコンテンツ鍵或いは上記復号化後のコンテンツ鍵を保管するコンテンツ鍵保管工程と、

上記加工されたディジタルコンテンツを上記コンテンツ鍵を用いて復号化するコンテンツ復号化工程と、

上記加工されたディジタルコンテンツを復号化する毎に減額される課金情報を要求するための課金情報要求情報を生成する課金情報要求情報生成工程と、

上記課金情報要求情報を暗号化して送信する課金情報要求情報送信工程と、

上記課金情報の要求に応じて送信されてきた課金情報を受信すると共に当該課金情報に施されている暗号化を復号化して格納する課金情報受信工程と、

上記加工されたディジタルコンテンツを伸長するコンテンツ伸長工程と、

上記加工されたディジタルコンテンツの復号化に応じたコンテンツ使用情報を生成して格納するコンテンツ使用情報格納工程と、

上記コンテンツ使用情報を暗号化して送信するコンテンツ使用情報送信工程とを有することを特徴とするディジタルコンテンツ再生方法。

【請求項１１】　コンテンツ使用情報格納工程では、上記格納されている課金情報の残高を確認し、上記加工されたディジタルコンテンツの復号化に応じて上記格納されている課金情報を減額し、少なくとも上記課金情報の減額量を含むコンテンツ使用情報を生成することを特徴とする請求項１０記載のディジタルコンテンツ再生方法。

【請求項１２】　上記復号化及び伸長がなされたディジタルコンテンツをディジタル／アナログ変換するディジタル／アナログ変換工程を有することを特徴とする請求項１０記載のディジタルコンテンツ再生方法。

【請求項１３】　上記コンテンツ受信工程では、上記加工されたディジタルコンテンツを外部記憶媒体に格納することを特徴とする請求項１０記載のディジタルコンテンツ再生方法。

【請求項１４】　上記コンテンツ鍵は共通鍵であることを特徴とする請求項１０記載のディジタルコンテンツ再生方法。

【請求項１５】　上記コンテンツ鍵復号化工程では、上

記コンテンツ鍵を固有の秘密鍵を用いて復号化することを特徴とする請求項１０記載のディジタルコンテンツ再生方法。

【請求項１６】　共通鍵を発生し、当該共通鍵を暗号化して送信する共通鍵送信工程を有することを特徴とする請求項１０記載のディジタルコンテンツ再生方法。

【請求項１７】　上記共通鍵送信工程では、上記共通鍵としてセッション鍵を生成することを特徴とする請求項１６記載のディジタルコンテンツ再生方法。

【請求項１８】　上記課金情報要求情報送信工程では、上記課金情報要求情報を上記共通鍵を用いて暗号化することを特徴とする請求項１６記載のディジタルコンテンツ再生方法。

【請求項１９】　上記コンテンツ使用情報送信工程では、上記コンテンツ使用情報の暗号化に上記共通鍵を用いることを特徴とする請求項１６記載のディジタルコンテンツ再生方法。

【請求項２０】　上記コンテンツ使用情報送信工程では、上記課金情報要求情報生成工程による上記課金情報の要求に伴って、上記暗号化したコンテンツ使用情報を送信することを特徴とする請求項１０記載のディジタルコンテンツ再生方法。

【請求項２１】　上記課金情報受信工程では、上記課金情報と共に暗号化されて送信されてくるコンテンツの使用条件を示す情報をも受信することを特徴とする請求項１０記載のディジタルコンテンツ再生方法。

【請求項２２】　データ通信を行うデータ通信手段と、暗号化及び圧縮処理によって加工されたディジタルコンテンツを受信して記憶媒体に記憶させるコンテンツ記憶制御手段と、
暗号化されたコンテンツ鍵を復号化するコンテンツ鍵復号化手段と、
上記暗号化されたコンテンツ鍵或いは上記復号化後のコンテンツ鍵を保管するコンテンツ鍵保管手段と、
上記加工されたディジタルコンテンツを上記コンテンツ鍵を用いて復号化するコンテンツ復号化手段と、
上記加工されたディジタルコンテンツを復号化する毎に減額される課金情報に施されている暗号化を復号化する課金情報復号化手段と、
上記復号化された課金情報を格納する課金情報格納手段と、
上記加工されたディジタルコンテンツを伸長するコンテンツ伸長手段と、
上記加工されたディジタルコンテンツの復号化に応じたコンテンツ使用情報を生成するコンテンツ使用情報生成手段と、
上記コンテンツ使用情報を格納するコンテンツ使用情報格納手段と、
上記コンテンツ使用情報を暗号化するコンテンツ使用情報暗号化手段とを有することを特徴とするディジタルコンテンツ再生装置。

【請求項２３】　上記加工されたディジタルコンテンツの復号化に必要なコンテンツ鍵を要求するためのコンテンツ鍵要求情報を暗号化するコンテンツ鍵要求情報暗号化手段と、
上記加工されたディジタルコンテンツを復号化する毎に減額される課金情報を要求するための課金情報要求情報を暗号化する課金情報要求情報暗号化手段とを有することを特徴とする請求項２２記載のディジタルコンテンツ再生装置。

【請求項２４】　コンテンツ使用情報生成手段は、上記課金情報格納手段に格納されている課金情報の残高を確認し、上記加工されたディジタルコンテンツの復号化に応じて、上記格納されている課金情報を減額し、少なくとも上記課金情報の減額量を含むコンテンツ使用情報を生成することを特徴とする請求項２２記載のディジタルコンテンツ再生装置。

【請求項２５】　上記復号化及び伸長がなされたディジタルコンテンツをディジタル／アナログ変換するディジタル／アナログ変換手段を有することを特徴とする請求項２２記載のディジタルコンテンツ再生装置。

【請求項２６】　上記コンテンツ記憶制御手段は、上記加工されたディジタルコンテンツを外部記憶媒体に記憶させることを特徴とする請求項２２記載のディジタルコンテンツ再生装置。

【請求項２７】　上記コンテンツ鍵は共通鍵であることを特徴とする請求項２２記載のディジタルコンテンツ再生装置。

【請求項２８】　装置固有の鍵を保管する固有鍵格保管段を有し、
上記コンテンツ鍵復号化手段では、上記固有鍵保管手段に保管している装置固有の秘密鍵を用いて、上記暗号化されているコンテンツ鍵を復号化することを特徴とする請求項２２記載のディジタルコンテンツ再生装置。

【請求項２９】　共通鍵を発生する共通鍵発生手段と、上記共通鍵を暗号化する共通鍵暗号化手段とを有することを特徴とする請求項２２記載のディジタルコンテンツ再生装置。

【請求項３０】　上記共通鍵発生手段は、上記共通鍵としてセッション鍵を生成することを特徴とする請求項２９記載のディジタルコンテンツ再生装置。

【請求項３１】　上記課金情報復号化手段は、上記課金情報を上記共通鍵を用いて復号化することを特徴とする請求項２９記載のディジタルコンテンツ再生装置。

【請求項３２】　上記コンテンツ使用情報暗号化手段は、上記コンテンツ使用情報を上記共通鍵を用いて暗号化することを特徴とする請求項２９記載のディジタルコンテンツ再生装置。

【請求項３３】　上記コンテンツ使用情報暗号化手段は、上記課金情報要求情報暗号化手段による上記課金情

報要求情報の暗号化に伴って、上記コンテンツ使用情報の暗号化を行うを有することを特徴とする請求項２２記載のディジタルコンテンツ再生装置。

【請求項３４】　上記課金情報復号化工程では、上記課金情報と共に暗号化されているコンテンツの使用条件を示す情報をも復号化することを特徴とする請求項２２記載のディジタルコンテンツ再生装置。

【請求項３５】　携帯可能に構成されてなることを特徴とする請求項２２記載のディジタルコンテンツ再生装置。

【請求項３６】　カード状の筐体を有することを特徴とする請求項２２記載のディジタルコンテンツ再生装置。

【請求項３７】　集積回路化してなることを特徴とする請求項２２記載のディジタルコンテンツ再生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、例えばオーディオデータやビデオデータ等のディジタルコンテンツを配布し、それらディジタルコンテンツの利用量に応じて課金するシステムに好適なディジタルコンテンツ配付管理方法、並びにディジタルコンテンツ再生方法及び装置に関する。

【０００２】

【従来の技術】コンピュータプログラムやオーディオデータ、ビデオデータ等のディジタルコンテンツの流通を簡便化し、潜在需要を掘り下げ、市場拡大に有利な手法としては、例えば特公平６－１９７０７号公報に記載されるソフトウェア管理方式、特公平６－２８０３０号公報に記載されるソフトウェア利用管理方式、特公平６－９５３０２号公報に記載されるソフトウェア管理方式のような手法が存在する。上記特公平６－１９７０７号公報に記載されたソフトウェア管理方式は、無体財産であるコンピュータプログラムやビデオデータ等のソフトウェアの利用に際し、ソフトウェアの利用状況をソフトウェア権利者別などによって把握できるようにしたものである。また、特公平６－２８０３０号公報に記載されるソフトウェア利用管理方式は、無体財産であるコンピュータプログラムやビデオデータ等のソフトウェアの利用に際し、有償プログラムを買い取り（買い取った後は無料で使用できる）価格を付し、コンピュータシステム内には購入可能な金額を示すデータを設けておき、有償プログラム購入の際は、同システムにある利用可能なソフトウェアの名称としてテーブルに登録すると共に、当該購入可能金額を示すデータをソフトウェア価格分だけ減じ、また登録済みソフトウェアを該テーブルから抹消する際には状況に応じて該購入可能な金額を示すデータを増加更新するようにしたものである。また、上記特公平６－９５３０２号公報に記載されるソフトウェア管理方式は、無体財産であるコンピュータプログラムやビデオデータ等のソフトウェアの利用に際し、有償プログラムにつき実際の利用量（利用回数または利用時間など）に応じて利用料金を徴収するために、利用されたプログラムの識別と「利用者識別符号と料金とを記録」しておき、該記録を回収することでプログラム権利者が自分の所有するプログラムの利用料金を把握でき、プログラムの利用量に応じたプログラム利用料金を回収する場合のシステムで有効なものである。

【０００３】

【発明が解決しようとする課題】ところが、上述したディジタルコンテンツをネットワークを使って配信するシステムは、パーソナルコンピュータ上だけでの運用を考慮しており、したがって、簡単に持ち運びができ、何時でも、また何処でも上記ディジタルコンテンツを楽しむといったシステムは存在しない。

【０００４】一方、上述した各公報記載の手法は、潜在需要を掘り下げ、市場拡大に有利であるが、ディジタルコンテンツのコピー或いは不当な使用への防御として不十分であり、且つ経済的なシステムとは言い難い。

【０００５】そこで、本発明はこのような状況に鑑みてなされたものであり、簡単に持ち運びができて何時でも何処でもディジタルコンテンツを楽しむことを可能とし、また、ディジタルコンテンツのコピー或いは不当な使用への防御として十分運用に耐え、且つ経済的なシステムを構築することをも可能にするディジタルコンテンツ配付管理方法、並びにディジタルコンテンツ再生方法及び装置を提供することを目的とする。

【０００６】

【課題を解決するための手段】本発明によれば、ディジタルコンテンツの配付側では、ディジタルコンテンツを暗号化及び圧縮して加工し、この加工したディジタルコンテンツと暗号化したコンテンツ鍵、さらに暗号化した課金情報を通信相手側に送信し、通信相手側から送信されてきたコンテンツ使用情報に基づいて徴収した利用金を権利者に対して分配するようにしており、一方、ディジタルコンテンツの再生側では、その加工されたディジタルコンテンツをコンテンツ鍵にて復号すると共に伸長して再生し、同時にコンテンツの使用に応じて課金情報の減額とコンテンツ使用情報の生成を行い、このコンテンツ使用情報を配付側に送信するようにし、また本発明のディジタルコンテンツ再生装置は、携帯可能となされていることにより、上述した課題を解決する。

【０００７】

【発明の実施の形態】以下、本発明の好ましい実施の形態について、図面を参照しながら説明する。

【０００８】先ず、本発明のディジタルコンテンツ配付方法、ディジタルコンテンツ再生方法及び装置の具体的内容及び構成の説明を行う前に、これらの理解を容易にするために、本発明が適用されるシステム全体の概略構成及びシステムの運用方法について図１から図７までの各図を用いて簡単に説明する。

【０００９】図１にはシステム全体の概略的な構成を示す。

【００１０】この図１において、ユーザ側２００は、本発明のディジタルコンテンツ再生装置（以下、プレーヤ１と呼ぶことにする）及びいわゆるパーソナルコンピュータ（以下、ユーザ端末５０と呼ぶことにする）を保有しているものとする。

【００１１】ユーザ端末５０は、通常のパーソナルコンピュータであるが、本発明に使用する後述する各種ソフトウェアをアプリケーションソフトとして格納してなると共に、表示手段であるディスプレイ装置と放音手段であるスピーカ、及び情報入力手段であるキーボードやマウス等が接続されてなるものである。当該ユーザ端末５０は例えばネットワークを介してシステム管理会社２１０と接続可能であり、また、プレーヤ１との間のインターフェイス手段を有し、データ送受が可能である。

【００１２】プレーヤ１は例えば図２に示すような構成を有するものである。

【００１３】この図２の構成の詳細な説明については後述するが、当該プレーヤ１は、ディジタルコンテンツの処理経路の主要構成要素として、暗号化されているディジタルコンテンツをコンテンツ鍵を用いて復号化する共通鍵暗号復号回路２４と、圧縮されているディジタルコンテンツを伸長する伸長手段である伸長回路２６と、ディジタルデータをアナログ信号に変換するＤ／Ａ変換回路２７とを少なくとも有する。なお、以下に言う復号化とは、暗号化を解くことである。

【００１４】また、このプレーヤ１は、使用するディジタルコンテンツの権利情報及び使用状況を示す情報（以下、これら情報をポイント使用情報と呼ぶ）や、ディジタルコンテンツを使用する際に必要となる保有金額データ、すなわちディジタルコンテンツを使用する毎に減額される課金データ（以下、ポイント情報と呼ぶ）等を扱う主要構成要素として、上記ポイント使用情報を格納するポイント使用情報格納メモリ２９と、上記ポイント情報を格納するポイント情報格納メモリ２８とを少なくとも備えている。

【００１５】さらに、このプレーヤ１は、後述するような暗号化及び復号化に使用する各種鍵を格納するための構成として共通鍵保管メモリ２２及び通信用鍵保管メモリ２１と、これらに格納された鍵を用いて暗号化や復号化を行うための構成として共通暗号復号回路２４及び公開暗号復号回路２０を有している。また、このプレーヤ１は、上記暗号化及び復号化に関連する構成として、システム管理会社２１０のホストコンピュータと連動した乱数を発生してセキュリティＩＤを生成するセキュリティＩＤ発生回路１９及びタイマ１８や、後述するいわゆるハッシュ値を発生するハッシュ関数回路２５等をも有している。

【００１６】その他、当該プレーヤ１は、ディジタルコンテンツやその他各種のデータ及び各構成要素の制御をＲ-ＯＭ１７に格納されたプログラムに基づいて行う制御手段であるコントローラ１６と、携帯時の動作電源としての電池５を備えている。

【００１７】ここで、図２のプレーヤ１の各主要構成要素は、セキュリティ上、ＩＣ（集積回路）或いはＬＳＩ（大規模集積回路）の１チップで構成されることが望ましい。この図２では、各主要構成要素が集積回路１０内に１チップ化されている。当該プレーヤ１には、外部とのインターフェイス用として３つの端子（アナログ出力端子２と、ＰＣ用インターフェイス端子３と、記録メディア用Ｉ／Ｏ端子４）を備え、これら各端子が集積回路１０のそれぞれ対応する端子１３、１２、１１に接続されている。なお、これら各端子は統合することも、また新たに別の端子を設けることも可能であり、特にこだわるものではない。

【００１８】システム管理会社２１０は、システム全体を管理する管理センタ２１１と、上記プレーヤ１を販売する販売店２１２とからなり、仮想店舗２３０を介してユーザ側２００のユーザ端末５０との間で、後述するようなディジタルコンテンツの供給に関する情報の送受、コンテンツプロバイダ２４０が保有するコンテンツを圧縮及び暗号化するディジタルコンテンツの加工、上記加工したディジタルコンテンツの供給、金融機関２２０との間の情報送受等を行う。なお、システム管理会社２１０と金融機関２２０との間では、ユーザ側２００の口座番号やクレジット番号，名前や連絡先等の確認や、ユーザ側２００との間で取引可能かどうかの情報等のやり取りなどが行われる。金融機関２２０とユーザ側２００との間では、実際の代金振込等の処理が行われる。また、販売店２１２は、必ずしもシステム管理会社２１０内に含まれる必要はなく、販売代理店であってもよい。

【００１９】上記システム管理会社２１０の管理センタ２１１は、例えば図３に示すような構成を有するものである。この図３の構成の詳細な説明については後述するが、主要構成要素として、ディジタルコンテンツを管理し、その展示、暗号化及び圧縮等の加工処理、ディジタルコンテンツの暗号化及び復号化に使用する鍵情報であるコンテンツ鍵やＩＤの発生等の各機能を有するコンテンツ管理機能ブロック１００と、ユーザ情報を管理し、通信文（メッセージやポイント情報等）の暗号化及び復号化、確認メッセージの発生、セキュリティＩＤの発生、金融機関２３０との間での決済申請、ポイントの発生等の各機能の他、ユーザ加入処理等を行うユーザ加入処理機能部１１８をも備えたユーザ管理機能ブロック１１０と、ポイント使用情報等を管理する使用情報管理機能ブロック１２０と、システム全体を管理し、通信機能を有する管理機能ブロック１３０とを、少なくとも有してなる。

【００２０】上述した図１のように構成されるシステム

の実際の運用方法の一例を、図４～図７を用いて説明する。なお、以下の運用方法は、ユーザ側２００やシステム管理会社２１０，金融機関２２０，コンテンツプロバイダ２４０等が実際に行う手順である。

【００２１】このシステムの運用方法の説明では、プレーヤ１の購入の手順、ディジタルコンテンツの検索からプレーヤ１用の記憶メディアに対するディジタルコンテンツのインストールまでの手順、当該ディジタルコンテンツを使用可能にするための課金用のポイント情報の購入と当該ディジタルコンテンツを使用した場合の精算の手順、ディジタルコンテンツの鑑賞に伴ってユーザから徴収した課金代金の分配の手順について順番に説明する。

【００２２】先ず、プレーヤ１の購入時の手順としては、図４の（１）及び（５）に示すように、ユーザ側２００が実際に店頭或いは通信販売等により、上記販売店２１２から上記プレーヤ１を購入する。

【００２３】このとき、上記販売店２１２は、図４の（２）に示すように、上記プレーヤ１の販売時に上記ユーザ側２００から提供された個人情報（名前や連絡先等）及び決済情報（銀行口座、クレジット番号等）と、上記販売したプレーヤ１固有の番号（プレーヤ固有鍵等を含む）とをシステム管理会社２１０の管理センタ２１１に登録する。

【００２４】管理センタ２１１は、図４の（３）に示すように、金融機関２２０に対して、上記ユーザ側２００から提供された口座番号やクレジット番号等の確認を行い、図４の（４）に示すように金融機関２２０から取引可能である旨の情報を得る。

【００２５】次に、ディジタルコンテンツの検索からプレーヤ１用の記憶メディアへのディジタルコンテンツのインストールまでの手順として、上記プレーヤ１を購入したユーザ側２００は、当該プレーヤ１とのインターフェイス手段を備えたユーザ端末５０を使って、図５の（１）に示すように、希望のディジタルコンテンツの検索，選択，編集，注文等を行う。このときの検索から注文までの処理は、ユーザ端末５０がアプリケーションソフトとして格納している検索ソフトを用い、例えばネットワークを介して接続された仮想店舗２３０に対して行う。

【００２６】仮想店舗２３０は、例えば管理センタ２１１がネットワーク上の仮想的に設けている店舗であり、この仮想店舗２３０には、例えば複数のコンテンツの内容を示す情報が展示されている。ユーザ側２００は、仮想店舗２３０にて提供されているこれらの情報に基づいて、所望のコンテンツの注文を行うことになる。なお、仮想店舗２３０に展示されるコンテンツの内容を示す情報としては、例えばコンテンツが映画等のビデオデータである場合には当該映画等のタイトルや広告、当該映画中の１シーン等の映像などが考えられ、また、コンテンツがオーディオデータである場合は曲名やアーティスト名、当該曲の最初の数フレーズ（いわゆるイントロ）等が考えられる。したがって、ユーザ側２００のユーザ端末５０にて上記仮想店舗２３０をアクセスした場合には、当該ユーザ端末５０上に上記仮想店舗２３０の複数のコンテンツの内容が仮想的に展示され、これら展示物の中から所望のものを選択することでコンテンツの注文が行われることとなる。

【００２７】上記ユーザ側２００のユーザ端末５０からディジタルコンテンツの注文等があったとき、上記仮想店舗２３０は、図５の（２）に示すように管理センタ２１１に対してディジタルコンテンツの供給依頼を行う。

【００２８】当該ディジタルコンテンツの供給依頼を受け取った管理センタ２１１は、コンテンツプロバイダ２４０に対して上記供給依頼のあったディジタルコンテンツの配給依頼を行う。これにより、当該コンテンツプロバイダ２４０は、図５の（４）に示すように上記配給依頼のあったディジタルコンテンツを管理センタ２１１に配給する。

【００２９】管理センタ２１１は、上記コンテンツプロバイダ２４０から配給されたディジタルコンテンツに対して暗号化及び所定の圧縮方式を用いた圧縮を施すと共に、この圧縮及び暗号化されたディジタルコンテンツに対して、当該コンテンツのＩＤ（コンテンツＩＤ）とこのコンテンツの著作権者等の権利者情報と当該コンテンツを使用したときの課金額とコンテンツをユーザ側２００に供給する仮想店舗名等とを付加する。なお、コンテンツに対する課金額は、コンテンツプロバイダ２４０にて事前に決定される。

【００３０】上記管理センタ２１１にて加工されたコンテンツは、図５の（５）に示すように、仮想店舗２３０に送られ、さらにこの仮想店舗２３０を介して、図５の（６）のようにユーザ側２００のユーザ端末５０に供給される。これにより、プレーヤ１には、上記ユーザ端末５０からコンテンツが供給され、このコンテンツが当該プレーヤ１に格納されることになる。

【００３１】なお、この図５に（２）～（５）までの流れについては、事前に行っておくことも可能である。すなわち、仮想店舗２３０には、上記複数のコンテンツの内容を示す情報を展示するだけでなく、これら展示に対応した上記加工されたディジタルコンテンツを予め用意しておくようにしても良い。

【００３２】次に、上述のようにしてプレーヤ１にインストールされたディジタルコンテンツを使用可能にするための課金用のポイント情報の購入と当該ディジタルコンテンツを使用した場合の精算の手順では、先ず、ユーザ端末５０によってプレーヤ１に格納されているポイント情報の不足が確認されて、当該ユーザ端末５０からポイント情報の補充要求がなされる。

【００３３】このとき、図６の（１）のように、当該ユ

ーザ端末５０からは、プレーヤ１にて暗号化されたポイント情報の補充依頼が、管理センタ２１１に対し転送される。また同時に、既に使用したディジタルコンテンツに対応する著作権者等の権利者の情報すなわちポイント使用情報がプレーヤ１から読み出されて暗号化され、ユーザ端末５０を介して管理センタ２１１に送られる。このように、ポイント情報の補充依頼と同時にポイント使用情報の転送が行われるようにしたのは、当該ポイント使用情報の管理センタ２１１への送信のみのために、ユーザ側２００が管理センタ２１１にアクセスする手間を省くためである。勿論、このポイント使用情報の転送は、必ずしもポイント情報の購入と同時に行う必要はなく、独立に行っても良い。

【００３４】上記暗号化されたポイント情報の補充依頼及びポイント使用情報を受け取った管理センタ２１１は、当該暗号を解読することでユーザ側２００が要求しているポイント情報の補充量とポイント使用情報の内容を認識する。さらに、当該管理センタ２１１は、金融機関２２０に対して図６の（２）のように当該ポイント補充分の決済が可能かどうかの確認を行う。金融機関２２０にて、ユーザ側２００の口座を調べることによって、決済可能であることが確認されると、当該金融機関２２０から図６の（３）のように決済ＯＫの指示が管理センタ２１１に送られることになる。

【００３５】また、このときの管理センタ２１１は、図６の（４）に示すように、コンテンツプロバイダ２４０に対して著作権者等の権利者に支払われることになるポイント使用数、すなわち金額を連絡する。

【００３６】その後、管理センタ２１１では、ポイント補充情報の命令書を暗号化し、これをセキュリティＩＤと共にポイント補充指示情報として、図６の（５）に示すようにユーザ端末５０に送る。このユーザ端末５０からプレーヤ１に送られた上記ポイント補充指示情報は、当該プレーヤ１において復号化され、さらにセキュリティＩＤの確認後に、ポイント情報格納メモリ２８へのポイント情報の補充と、ポイント使用情報格納メモリ２９からの上記先に連絡した著作権情報等の権利者情報の削除とが行われる。

【００３７】次に、ディジタルコンテンツの鑑賞に伴ってユーザから徴収した課金代金、すなわちポイントの使用情報に応じてユーザの口座から引き落とされることになる代金の分配の手順では、先ず図７の（１）のようにユーザ側２００に対して代金振り込み依頼が金融機関２２０からなされる。このとき、ユーザ側２００の口座に十分な残高がある場合には、特に代金振り込み依頼はなされず、口座に十分な残高がない場合には、図７の（２）のようにユーザ側２００から金融機関２２０に対して代金の振り込みがなされる。

【００３８】金融機関２２０は、所定の手数料を差し引いて、図７の（３）のように、ユーザ側２００から受け取った代金を管理センタ２１１に対して送金する。すなわち管理センタ２１１では、金融機関２２０から送金された上記代金から、コンテンツ加工料と金融手数料とシステム管理費等を徴収する。また、当該管理センタ２１１は、先に使用されたポイントに応じた著作権料を、図７の（４）のようにコンテンツプロバイダ２４０に対して支払うと共に、仮想店舗２３０に対しては図７の（５）のように店舗手数料を支払う。上記著作権料を受け取ったコンテンツプロバイダ２４０は著作権料を各著作権者に支払い、上記店舗手数料を受け取った仮想店舗２３０は仮想店舗毎の手数料を各仮想店舗に対して支払う。

【００３９】このように、ユーザ側２００から支払われた代金は、前記ポイント使用情報に基づいて、著作権料と店舗手数料とコンテンツ加工手数料と決済手数料とシステム管理手数料とに分配され、上記著作権料はコンテンツプロバイダ２４０に、上記店舗手数料は上記仮想店舗２３０に、コンテンツ加工手数料はシステム管理会社２１０に、決済手数料はシステム管理会社と金融機関２２０に、システム管理手数料はシステム管理会社２１０に支払われる。

【００４０】ここで、本実施の形態のシステム間でのデータ送受、すなわち管理センタ２１１とプレーヤ１との間のデータ送受の際には、データ通信の安全性を確保するために、通信するデータの暗号化及び復号化が行われる。本発明実施の形態では、暗号化及び復号化の方式として共通鍵暗号方式及び公開鍵暗号方式の何れにも対応可能となっている。

【００４１】本発明の実施の形態では、上記ディジタルコンテンツ、上記ポイント使用情報、ポイント情報、メッセージやセキュリティＩＤ、その他の各種情報の伝送の際の暗号方式としては、処理速度の点から共通鍵暗号方式を採用している。これら各種情報の暗号化及び復号化に使用する共通鍵は、それぞれ各情報に対応して異なるものである。前記図２のプレーヤ１では、管理センタ２１１から伝送されてくる暗号化された情報の復号化に使用する共通鍵が前記共通鍵保管メモリ２２に保管され、この共通鍵保管メモリ２２に保管している共通鍵を用いて、前記共通暗号復号回路２４が、上記管理センタ２１１からの暗号化された情報の復号化を行う。

【００４２】一方、上記各種情報の暗号化や復号化に使用する上記共通鍵の伝送の際の暗号方式としては、前記プレーヤ１の固有の鍵であるプレーヤ固有鍵が何れの方式に対応しているかによって採用される暗号方式が変わるものである。すなわち、上記プレーヤ固有鍵が共通鍵暗号方式に対応している場合、上記共通鍵は当該プレーヤ固有鍵を用いて暗号化され、また当該暗号化された共通鍵は上記プレーヤ固有鍵を用いて復号化されることになる。これに対して、上記プレーヤ固有鍵が公開鍵暗号方式に対応している場合、上記共通鍵の暗号化には相手

先の公開鍵が用いられ、暗号化された上記共通鍵の復号化にはそれぞれ復号化を行う側の秘密鍵が用いられる。

【００４３】例えば上記プレーヤ１から管理センタ２１１に上記共通鍵（例えば後述するセッション鍵）が送られる場合において、上記プレーヤ固有鍵が共通鍵暗号方式に対応しているときには、上記プレーヤ１では通信用鍵保管メモリ２１が保管しているプレーヤ固有鍵を用いて上記共通鍵暗号復号回路２４が上記共通鍵を暗号化し、管理センタ２１１では当該管理センタ２１１が保管しているプレーヤ固有鍵を用いて、上記暗号化されてる共通鍵の復号化を行う。同じく、上記プレーヤ１から管理センタ２１１に上記共通鍵が送られる場合において、例えば上記プレーヤ固有鍵が公開鍵暗号方式に対応しているときには、上記プレーヤ１の通信用鍵保管メモリ２１が保管している管理センタ２１１の公開鍵にて上記公開鍵暗号復号回路２０が上記共通鍵を暗号化し、管理センタ２１１では当該管理センタ２１１が保管している秘密鍵を用いて、上記暗号化されてる共通鍵の復号化を行う。

【００４４】逆に、例えば上記管理センタ２１１からプレーヤ１に上記共通鍵（例えばコンテンツ鍵）が送られる場合において、上記プレーヤ固有鍵が共通鍵暗号方式に対応しているときには、上記管理センタ２１１が保管しているプレーヤ固有鍵にて上記共通鍵が暗号化され、プレーヤ１では上記通信用鍵保管メモリ２１にて保管しているプレーヤ固有鍵を用いて、前記共通暗号復号回路２４が上記暗号化されてる共通鍵の復号化を行う。同じく、上記管理センタ２１１からプレーヤ１に上記共通鍵が送られる場合において、例えば上記プレーヤ固有鍵が公開鍵暗号方式に対応しているときには、上記管理センタ２１１が保管しているプレーヤ１の公開鍵にて上記共通鍵が暗号化され、プレーヤ１では上記通信用鍵保管メモリ２１にて保管しているプレーヤ固有鍵すなわち秘密鍵を用いて、前記公開暗号復号回路２０が上記暗号化されてる共通鍵の復号化を行う。

【００４５】上述したようなプレーヤ固有鍵自身の暗号方式は、当該プレーヤ固有鍵の配送（システム管理会社２１０からプレーヤ１への配送）が容易か否かによって決定されている。すなわち、コスト的には共通鍵暗号方式の方が有利であるので、プレーヤ固有鍵の配送が容易であれば共通鍵暗号方式を採用するが、当該プレーヤ固有鍵の配送が困難であるときにはコスト高であるが公開鍵暗号方式を採用する。プレーヤ固有鍵をハードウェアに実装する場合には共通鍵暗号方式を、ソフトウェアに実装する場合には公開鍵暗号方式を採用する。

【００４６】以下、本発明の実施の形態では、プレーヤ固有鍵自身の暗号方式としてソフトウェアに実装する場合の互換性を考慮して、上記公開鍵暗号方式を採用する例を挙げて説明することにする。すなわち、上記管理センタ２１１とプレーヤ１との間で前記共通鍵の伝送が行

われる場合において、上記プレーヤ１側で共通鍵（セッション鍵）が暗号化されるときには管理センタ２１１の公開鍵を用いて暗号化がなされ、管理センタ２１１では上記プレーヤ固有鍵（すなわち秘密鍵）を用いて上記暗号化されてる共通鍵の復号化を行う。逆に、上記管理センタ２１１側で共通鍵（コンテンツ鍵）が暗号化されるときには、プレーヤの公開鍵にて暗号化がなされ、プレーヤ１では上記プレーヤ固有鍵（すなわち秘密鍵）を用いて上記暗号化されてる共通鍵の復号化を行う。

【００４７】前述したような各手順と暗号方式を用いて運用されるシステムを構成する上記プレーヤ１とユーザ端末５０と管理センタ２１１の実際の動作を、以下に順番に説明する。

【００４８】先ず、上述したポイント補充すなわちポイント購入時のプレーヤ１、ユーザ端末５０、管理センタ１０における処理の流れについて、図８から図１１を用い、前記図２及び図３を参照しながら説明する。

【００４９】図８には、ポイントを購入する際のプレーヤ１における処理の流れを示している。

【００５０】この図８において、ステップＳＴ１では、ユーザ端末５０すなわちパーソナルコンピュータに予めインストールされているポイント購入用のソフトウェアの立ち上げが行われ、この間のプレーヤ１のコントローラ１６は、当該ポイント購入用のソフトウェアが立ち上がるまで待っている。

【００５１】上記ポイント購入用のソフトウェアが立ち上がると、ステップＳＴ２にて、プレーヤ１のコントローラ１６は、上記ユーザ端末５０に入力された情報を、当該ユーザ端末５０から受信する。このときのユーザ端末５０に入力される情報とは、上記ポイント購入用のソフトウェアに従って、上記ユーザ端末５０を操作するユーザに対して当該ユーザ端末５０から入力要求がなされるものであり、例えばパスワードや購入したいポイント情報数等の情報である。

【００５２】これらユーザ端末５０からの情報は、プレーヤ１のＰＣ用インターフェース端子３及び当該プレーヤ１内に１チップ化された集積回路１０の端子１２を介して、コントローラ１６に受信される。当該ユーザ端末５０からの情報を受信したコントローラ１６は、ステップＳＴ３にて、当該プレーヤ１の集積回路１０内のパスワード格納メモリ１４が格納するパスワードと、上記受信した情報中のパスワードとの比較を行い、上記受信パスワードが正しいかどうかの確認を行う。

【００５３】上記パスワードが正しいと確認したコントローラ１６は、ステップＳＴ４にて、ポイントを購入したい旨の情報（ポイント購入の主旨）と購入したいポイント情報数その他の情報を生成すると同時に、セキュリティＩＤ発生回路１９からセキュリティＩＤを発生させ、次のステップＳＴ５にてこれらの情報を共通暗号復号回路２４にて暗号化させる。コントローラ１６は、次

にステップＳＴ６にて、ユーザＩＤ格納メモリ２３からユーザＩＤを読み出し、当該ユーザＩＤを上記暗号化した情報に付加し、さらに、ステップＳＴ７にて、当該ユーザＩＤを付加して作成したデータを上記端子１２及びＰＣ用インターフェース端子３を介してユーザ端末５０に転送する。このユーザ端末５０からは、上記作成データが管理センタ２１１に送られることになる。

【００５４】このとき、上記作成データの暗号化には前述したように共通鍵暗号方式が採用されているため、当該作成データの伝送に先立ち、共通鍵の生成が行われる。このため、上記コントローラ１６では、上記共通鍵として、例えば乱数発生手段であるセキュリティＩＤ発生回路１９からセッション鍵を発生させる。また、この共通鍵（セッション鍵）は、上記作成データの伝送に先だって、プレーヤ１から管理センタ２１１に対して送られることになる。ここで、当該共通鍵は前述のように公開鍵暗号方式にて暗号されるものであるため、上記コントローラ１６では、上記共通鍵であるセッション鍵を公開暗号復号回路２０に送ると同時に、通信用鍵保管メモリ２１に予め保管されている管理センタ２１１の公開鍵を取り出して上記公開暗号復号回路２０に送る。これにより当該公開暗号復号回路２０では、上記管理センタ２１１の公開鍵を用いて上記共通鍵（セッション鍵）の暗号化が行われる。このようにして暗号化されたセッション鍵はユーザＩＤと共に、上記作成データの伝送に先だって管理センタ２１１に送られている。

【００５５】なお、前述したように、ポイント情報の要求と共にポイント使用情報の転送も行う場合、コントローラ１６は、ポイント使用情報格納メモリ２９から前記権利者情報等を含むポイント使用情報を読み出し、これらも上記共通暗号復号回路２６に送って暗号化させる。この暗号化したポイント使用情報は、上記作成データと共に伝送される。また、ポイント使用情報の転送と同時に、ポイント情報の残高なども同様にして転送することも可能である。

【００５６】その後、コントローラ１６は、ステップＳＴ８にて、ユーザ端末５０を通して管理センタ２１１から送られてきた暗号化されているデータを受信する。この管理センタ２１１から送られてきたデータは、先に当該プレーヤ１から転送した上記購入したいポイント情報数に応じたポイント情報とセキュリティＩＤ等の情報が、上記セッション鍵と同じ共通鍵を用いて暗号化されたデータである。

【００５７】コントローラ１６は、上記管理センタ２１１からのデータを受信すると、ステップＳＴ９にて、当該データを上記共通暗号復号回路２４に送ると共に、先に発生して共通鍵保管メモリ２２に保管しておいた前記共通鍵を読み出して同じく共通暗号復号回路２４に送る。当該共通暗号復号回路２４では、上記共通鍵を用いて上記管理センタ２１１からの暗号化されたデータを復号化する。

【００５８】次に、上記コントローラ１６は、ステップＳＴ１０にて、上記復号化されたデータのセキュリティＩＤを、上記セキュリティＩＤ発生回路１９からのセキュリティＩＤとの比較によって確認し、その確認後、ステップＳＴ１１にて、上記ポイント情報格納メモリ２８に格納されていたポイント情報を、上記新たに送られてきたポイント情報にて修正する。

【００５９】上記ポイント情報の修正等の処理が終了すると、コントローラ１６は、ステップＳＴ１２にて、処理完了のサインを生成して、上記共通鍵保管メモリ２２から読み出した共通鍵と共に上記共通暗号復号回路２４に送り、当該共通暗号復号回路２４にて暗号化させる。その後、コントローラ１６は、ステップＳＴ１３にて当該暗号化された処理完了のサインを、端子１２及び３を介してユーザ端末５０に転送し、管理センタ２１１に送る。

【００６０】以上により、ポイント購入の際のプレーヤ１における処理の流れが終了する。

【００６１】次に、上記ポイント購入時のユーザ端末５０における処理の流れを、図９を用いて説明する。

【００６２】この図９において、ユーザ端末５０は、ステップＳＴ２１にて、ポイント購入用のソフトウェアの立ち上げを行う。当該ポイント購入用ソフトウェアが立ち上がると、このユーザ端末５０では、ステップＳＴ２２にて、上記ポイント購入用のソフトウェアに従い当該ユーザ端末５０を操作するユーザに対して上述したパスワードや購入したいポイント数等の情報の入力要求を行い、ユーザからこれらの情報が入力されると、当該入力された情報を前記図８のステップＳＴ２のように上記プレーヤ１に転送する。

【００６３】次に、ユーザ端末５０は、ステップＳＴ２３にて、上記プレーヤ１から前記図８のステップＳＴ７のように作成されたデータを受信すると、ステップＳＴ２４にて、当該プレーヤ１から転送されたデータを、予め登録されているアドレスすなわち管理センタ２１１へ転送する。

【００６４】上記データの転送を行った後のユーザ端末５０は、管理センタ２１１からの返送を待ち、管理センタ２１１からのデータ返送があると、ステップＳＴ２５にて当該管理センタ２１１からのデータをそのままプレーヤ１に転送する。

【００６５】当該ユーザ端末５０は、ステップＳＴ２６にて、上記プレーヤ１から前記図８のステップＳＴ１３のように処理完了のサインを受信すると、当該ポイント購入等の処理が終了したことをユーザに知らせるために、ステップＳＴ２７にて処理完了のサインをディスプレイに表示し、ユーザに確認させる。

【００６６】その後、当該ユーザ端末５０は、上記プレーヤ１から送られてきた処理完了のサインの暗号文を管

理センタ２１１に転送する。

【００６７】以上により、ポイント購入の際のユーザ端末５０における処理の流れが終了する。

【００６８】次に、ポイント購入時の管理センタ２１１における処理の流れを、図１０を用いて説明する。

【００６９】この図１０において、管理センタ２１１は、ステップＳＴ３１のように、コントロール機能部１３１にて全体が制御される管理機能ブロック１３０の通信機能部１３３によって、前記図８のステップＳＴ７及び図９のステップＳＴ２４のようにユーザ端末５０を介して転送されたプレーヤ１からの上記暗号化されたデータを受信する。このデータを受信すると、管理センタ２１１のユーザ管理機能ブロック１１０は、ステップＳＴ３２のように、コントロール機能部１１１の制御の元で、当該受信したデータに添付されたユーザＩＤに基づいて、データベース部１１２から共通鍵を入手すると共にセキュリティＩＤ発生機能部１１６からセキュリティＩＤを入手する。

【００７０】なお、この時の共通鍵は、前記プレーヤ１から予め送られてきている前記セッション鍵であり、このセッション鍵は前述のように公開鍵暗号方式にて暗号化されて送られてきたものである。したがって、この暗号化されているセッション鍵の復号時には、当該管理センタ２１１のユーザ管理機能ブロック１１０において、上記管理センタ２１１の公開鍵暗号方式の秘密鍵が取り出され、この秘密鍵と上記暗号化されているセッション鍵とが通信文暗号／復号機能部１１４に送られる。当該通信文暗号／復号機能部１１４では、上記管理センタ２１１の公開鍵を用いて上記暗号化されたセッション鍵の復号化が行われる。このようにして得られたセッション鍵（共通鍵）が上記データベース部１１２に格納されている。

【００７１】上記データベース部１１２から上記ユーザＩＤに対応する共通鍵を入手すると共にセキュリティＩＤ発生機能部１１６からセキュリティＩＤを入手すると、ステップＳＴ３３に示すように、管理センタ２１１のユーザ管理機能ブロック１１０の通信文暗号／復号機能部１１４において、上記共通鍵を用いて、上記プレーヤ１からの上記暗号化されたデータの復号化を行い、さらにコントロール機能部１１１において、当該復号化したデータ中のセキュリティＩＤと上記セキュリティＩＤ発生機能部１１６から読み出したセキュリティＩＤとの比較によって、アクセスしてきたユーザ側２００（プレーヤ１）が正当な使用者であるかどうかの内容確認を行う。

【００７２】上記アクセス元の正当性を確認した管理センタ２１１では、ステップＳＴ３４のように、ユーザ管理機能ブロック１１０のポイント発生機能部１１３にて、上記ユーザ端末５０から送られてきたデータの内容に応じたポイント情報の発行を行い、また、決済請求機能部１１７にて、ユーザの決済機関（金融機関２２０）への請求準備を行う。

【００７３】さらに、管理センタ２１１は、ステップＳＴ３５のように、例えばコントロール機能部１１１において、プレーヤ１からのポイント情報の残高とポイント使用情報に不正が無いことを確認し、後の処理のために情報のまとめを行う。すなわち、ポイント情報の残高と実際に使用したポイント情報の数とから不正な使用がないかどうかの確認とまとめとを行う。なお、この確認とまとめは、必ず行わなければならないものではないが、望ましくは行った方が良い。

【００７４】管理センタ２１１のユーザ管理機能ブロック１１０ではまた、上記ステップＳＴ３５の処理の後、ステップＳＴ３６のように、セキュリティＩＤ発生機能部１１５において上記プレーヤ１（ユーザ）への新たなセキュリティＩＤを例えば乱数発生に基づいて算出し、さらに、例えばコントロール機能部１１０にて、上記セキュリティＩＤを上記ポイント情報と共に暗号化する。このときの暗号化も前記プレーヤ１から予め送られてきている前記セッション鍵（共通鍵）を用いて行う。

【００７５】上記暗号化が終了すると、管理センタ２１１の管理機能ブロック１３０の通信機能部１３３では、コントロール機能部１３１の制御の元、上記暗号化したデータを前記図９のステップＳＴ２５及び図８のステップＳＴ８のようにユーザ端末５０を介してプレーヤ１に転送する。

【００７６】その後、管理センタ２１１の通信機能部１３３において、ステップＳＴ３８のように、前記図９のステップＳＴ２８に示したユーザ端末５０からの処理完了サインを受信して復号化すると、管理センタ２１１のユーザ管理機能ブロック１１０の決済請求機能部１１７では、ステップＳＴ３９のように、当該処理完了サインに基づいて金融機関２２０に決済を請求する。この金融機関２２０に対する決済請求は、管理機能ブロック１３０の通信機能部１３２から行われる。

【００７７】以上により、ポイント購入の際の管理センタ２１１における処理の流れが終了する。

【００７８】上述した図８から図１０の処理の流れにおけるプレーヤ１とユーザ端末５０と管理センタ２１１との間の情報送受のシーケンスは、図１１に示すように表すことができる。

【００７９】すなわちこの図１１において、入力情報転送Ｔ１では、前記図８のステップＳＴ２及び図９のステップＳＴ２２のように、ユーザ端末５０からプレーヤ１に対して、前記パスワードやポイント数等の入力情報が転送される。

【００８０】作成データ転送Ｔ２では、前記図８のステップＳＴ７及び図９のステップＳＴ２３のように、プレーヤ１からユーザ端末５０に対して、前記プレーヤ１にて作成したデータが転送される。また、データ転送Ｔ３

では、前記図９のステップＳＴ２４及び図１０のステップＳＴ３１のように、ユーザ端末５０から管理センタ２１１に対して、前記プレーヤ１が作成したデータが転送される。

【００８１】データ転送Ｔ４では、前記図１０のステップＳＴ３７及び図９のステップＳＴ２５のように、管理センタ２１１からユーザ端末５０に対して、管理センタ２１１にて暗号化したデータが転送される。また、転送Ｔ５では、前記図９のステップＳＴ２５及び図８のステップＳＴ８のように、管理センタ２１１からのデータをユーザ端末５０がそのままプレーヤ１に転送される。

【００８２】処理完了サイン転送Ｔ６では、前記図８のステップＳＴ１３及び図９のステップＳＴ２６のように、プレーヤ１からの処理完了サインがユーザ端末５０に転送される。さらに、処理完了サイン暗号文転送では、前記図９のステップＳＴ２８及び図１０のステップＳＴ３８のように、プレーヤ１からの暗号化された処理完了サインが管理センタ２１１に転送される。

【００８３】次に、上述したディジタルコンテンツの入手時のプレーヤ１、ユーザ端末５０、管理センタ２１１における処理の流れについて、図２及び図３を参照しながら、図１２から図１５を用いて説明する。

【００８４】図１２には、ディジタルコンテンツの入手時のプレーヤ１における処理の流れを示している。

【００８５】この図１２において、コントローラ１６は、ステップＳＴ４１のように、ユーザ端末５０すなわちパーソナルコンピュータに予めインストールされているディジタルコンテンツ入手用のソフトウェアの立ち上げが行われるまで待っている。

【００８６】上記ディジタルコンテンツ入手用のソフトウェアが立ち上がると、コントローラ１６は、ステップＳＴ４２のように、ユーザ端末５０を介して管理センタ２１１からディジタルコンテンツを含むデータを受信する。このときユーザ端末５０から端子３及び１２を介して受信するデータは、前述したようにコンテンツ鍵（コンテンツ毎に異なる共通鍵）で暗号化されたディジタルコンテンツと、当該ディジタルコンテンツに対応するコンテンツＩＤとを少なくとも有してなる。したがって、この暗号化されたディジタルコンテンツを使用するには、コンテンツ鍵を管理センタ２１１から入手しなければならない。このコンテンツ鍵の入手の方法については後述する。

【００８７】このユーザ端末５０からのデータを受信したコントローラ１６は、このデータすなわち暗号化されたディジタルコンテンツを、集積回路１０の端子１１を介し、記憶メディア用Ｉ／Ｏ端子４に接続されている記憶メディアに格納する。なお、この記憶メディアとしては、書き換え可能な光ディスクや半導体メモリ等の各種の記憶媒体が考えられるが、ランダムアクセス可能なものが望ましい。

【００８８】以上により、ディジタルコンテンツの入手時のプレーヤ１における処理の流れが終了する。

【００８９】次に、ディジタルコンテンツの入手時のユーザ端末５０における処理の流れを、図１３を用いて説明する。

【００９０】この図１３において、ユーザ端末５０は、ステップＳＴ５１にて、ディジタルコンテンツ入手用のソフトウェアの立ち上げを行う。当該ソフトウェアが立ち上がると、このユーザ端末５０では、ステップＳＴ５２にて、上記ディジタルコンテンツ入手用のソフトウェアに従い、予め登録されているアドレスの管理センタ２１１にアクセスする。

【００９１】このとき、当該管理センタ２１１は、前記仮想店舗２３０を用いて複数のディジタルコンテンツを展示している。ユーザ端末５０からは、ステップＳＴ５３にて、この仮想店舗２３０に展示されている複数のディジタルコンテンツのなかから、ユーザの選択操作に応じた所望のディジタルコンテンツが指定される。すなわち、ユーザ端末５０は、ステップＳＴ５４のように、仮想店舗２３０に展示されたディジタルコンテンツの中の所望のディジタルコンテンツを指定するためのコンテンツの指定情報を管理センタ２１１に送信する。

【００９２】ステップＳＴ５５のように、上記コンテンツ指定情報に応じて管理センタ２１１から返送されたデータ、すなわち前記暗号化されたディジタルコンテンツ及びコンテンツＩＤからなるデータを受信すると、当該ユーザ端末５０は、ステップＳＴ５６のように、内部の例えばハードディスクやメモリ等の格納手段に上記データを一旦格納する。

【００９３】その後、ユーザ端末５０は、当該格納したデータ（暗号化されたディジタルコンテンツ及びコンテンツＩＤ）を、前記図１２のステップＳＴ４２のようにプレーヤ１に転送する。

【００９４】以上により、ディジタルコンテンツの入手時のユーザ端末５０における処理の流れが終了する。

【００９５】次に、ディジタルコンテンツ入手時の管理センタ２１１における処理の流れを、図１４を用いて説明する。

【００９６】ここで、図３に示す管理センタ２１１は、前述した仮想店舗２３０に複数のコンテンツを展示させている。具体的には、管理センタ２１１のコンテンツ管理機能ブロック１００において、前記仮想店舗２３０を生成しており、この仮想店舗２３０に上記複数のディジタルコンテンツの展示を行っている。

【００９７】このように仮想店舗２３０にディジタルコンテンツを展示している状態で、図１４のステップＳＴ６１のように、前記図１３のステップＳＴ５４にてユーザ端末５０からコンテンツ指定情報を受信する。

【００９８】当該ユーザ端末５０から上記コンテンツ指定情報を受信すると、コンテンツ管理機能ブロック１０

０のコントロール機能部１０１は、このコンテンツ指定情報を管理機能ブロック１３０に送る。管理機能ブロック１３０のコントロール機能部１３１は、上記コントロール管理機能ブロック１００から受け取ったコンテンツ指定情報を、権利者用の通信機能部１３４を通して、前記コンテンツプロバイダ２４０に転送する。これにより当該コンテンツプロバイダ２４０からは、上記コンテンツ指定情報にて要求されたディジタルコンテンツが転送されてくる。上記コンテンツプロバイダ２４０から入手したディジタルコンテンツは、管理機能ブロック１３０からコンテンツ管理機能ブロック１００に送られ、このコンテンツ暗号・圧縮化機能部１０４に入力される。このとき、コントロール機能部１０１は、コンテンツ鍵・ＩＤ発生機能部１０３にて発生されてデータベース１０２に格納されているコンテンツ鍵を、上記コンテンツ暗号・圧縮化機能部１０４に送る。このコンテンツ暗号・圧縮化機能部１０４では、上記ディジタルコンテンツに対して上記コンテンツ鍵を用いた暗号化を施し、さらに所定の圧縮処理を施す。コントロール機能部１０１は、上記暗号化及び圧縮処理されたディジタルコンテンツに対して、データベース１０２から取り出したコンテンツＩＤを付加し、管理機能ブロック１３０に送る。なお、ディジタルコンテンツがオーディオ信号である場合の所定の圧縮処理としては、例えば近年製品化されているいわゆるＭＤ（ミニディスク：商標）にて使用されている技術である、いわゆるＡＴＲＡＣ（Adaptive TRansform Acoustic Coding）のように、人間の聴覚特性を考慮してオーディオデータを高能率圧縮する処理を一例として挙げることができる。

【００９９】その後、図１４のステップＳＴ６２に示すように、管理機能ブロック１３０のコントロール部１３１は、ユーザ端末との通信機能部１３３を通して、上記暗号化及び圧縮処理されてコンテンツＩＤが付加されたディジタルコンテンツを、上記ユーザ端末５０に送信する。

【０１００】ディジタルコンテンツ入手時の管理センタ２１１における処理の流れは以上である。

【０１０１】上述した図１２から図１４の処理の流れにおけるプレーヤ１とユーザ端末５０と管理センタ２１１との間の情報送受のシーケンスは、図１５に示すように表すことができる。

【０１０２】すなわちこの図１５において、入力情報転送Ｔ１１では、前記図１３のステップＳＴ５４のように、ユーザ端末５０から管理センタ２１１に対して、前記コンテンツ指定情報が転送される。コンテンツ転送Ｔ１２では、管理センタ２１１から、前記図１４のステップＳＴ６２のように、暗号化されたディジタルコンテンツとコンテンツＩＤがユーザ端末５０に転送される。

【０１０３】コンテンツ転送Ｔ１３では、前記図１３のステップＳＴ５７及び図１２のステップＳＴ４２のように、ユーザ端末５０に一旦格納された上記暗号化されたディジタルコンテンツとコンテンツＩＤがプレーヤ１に転送される。

【０１０４】次に、上述したディジタルコンテンツを使用する際に必要となるコンテンツ鍵とその使用条件の入手時のプレーヤ１、ユーザ端末５０、管理センタ２１１における処理の流れについて、図２及び図３を参照しながら、図１６から図１９を用いて説明する。

【０１０５】図１６には、コンテンツ鍵及び使用条件の入手時のプレーヤ１における処理の流れを示している。

【０１０６】この図１６のステップＳＴ７１では、プレーヤ１のコントローラ１６において、ユーザ端末５０に予めインストールされているコンテンツ鍵及び使用条件入手用のソフトウェアの立ち上げが行われるまで待っている。

【０１０７】上記ユーザ端末５０の上記コンテンツ鍵及び使用条件入手用のソフトウェアが立ち上がると、当該ソフトウェアに従ってユーザ端末５０に入力された情報が、ステップＳＴ７２のように、前記ＰＣ用インターフェース端子３及び集積回路１０の端子１２を介して受信される。このときの上記ユーザ端末５０から供給される入力情報は、鑑賞したいディジタルコンテンツの暗号化を解くのに必要なコンテンツ鍵を要求するための情報である。なお、この例では、上記コンテンツ鍵の要求情報として、このコンテンツ鍵を使用するディジタルコンテンツの指定情報を用いている。

【０１０８】このコンテンツ指定情報を上記ユーザ端末５０から受信したコントローラ１６は、ステップＳＴ７３にて、当該コンテンツ指定情報にて指定されたディジタルコンテンツのＩＤと、セキュリティＩＤ発生回路１９からのセキュリティＩＤとを作成し、この作成したデータを共通暗号復号回路２４にて暗号化させる。また、コントローラ１６は、当該作成したデータにユーザＩＤ格納メモリ２３から読み出したユーザＩＤを付加し、上記端子１２及びＰＣ用インターフェース端子３を介してユーザ端末５０に転送する。このユーザ端末５０からは、上記作成データが管理センタ２１１に送られることになる。

【０１０９】このときの作成データの暗号化にも、前述したように共通鍵暗号方式が採用されているため、当該作成データの伝送に先立ち、共通鍵の生成が行われる。このため、上記コントローラ１６では、上記共通鍵として、例えば乱数発生手段であるセキュリティＩＤ発生回路１９からセッション鍵を発生させる。また、この共通鍵（セッション鍵）は、上記作成データの伝送に先だって、プレーヤ１から管理センタ２１１に対して送られることになる。当該共通鍵は、前述のように公開鍵暗号方式にて暗号されるものであるため、上記コントローラ１６では、上記共通鍵であるセッション鍵を公開暗号復号回路２０に送ると同時に、通信用鍵保管メモリ２１に予

め保管されている管理センタ２１１の公開鍵を取り出して上記公開暗号復号回路２０に送る。これにより当該公開暗号復号回路２０では、上記管理センタ２１１の公開鍵を用いて上記共通鍵（セッション鍵）の暗号化が行われる。このようにして暗号化されたセッション鍵が、上記作成データの伝送に先だって管理センタ２１１に送られている。

【０１１０】その後、コントローラ１６は、ステップＳＴ７５にて、後述するようにユーザ端末５０を介して管理センタ２１１から送付されてきた暗号化されたデータを受信する。このときの管理センタ２１１から送られてきたデータは、後述するように上記コンテンツ鍵と使用条件とセキュリティＩＤ等が暗号化されたものである。

【０１１１】上記管理センタ２１１からの暗号化されたデータを受信すると、プレーヤ１では、ステップＳＴ７６のように、上記暗号化されたデータを復号化すると共にそのデータの正当性の確認を行う。すなわち、コントローラ１６は、上記復号化されたデータのセキュリティＩＤを、上記セキュリティＩＤ発生回路１９からのセキュリティＩＤとの比較によって確認することによる正当性の評価を行う。

【０１１２】ここで、コンテンツ鍵については後述するように公開鍵暗号方式にて暗号化がなされ、使用条件及びセキュリティＩＤについては共通鍵暗号方式にて暗号化がなされている。したがって、当該暗号化されているコンテンツ鍵を復号化するには、公開鍵暗号方式の秘密鍵が必要であり、本実施の形態のプレーヤ１では前述したようにプレーヤ固有鍵を秘密鍵として使用することにしているので、当該プレーヤ固有鍵が通信用鍵保管メモリ２１から取り出される。このプレーヤ固有鍵は、上記暗号化されたコンテンツ鍵と共に公開暗号復号回路２０に送られる。この公開暗号復号回路２０では、上記暗号化されているコンテンツ鍵を上記プレーヤ固有鍵を用いて復号化する。このように復号化されたコンテンツ鍵は、共通鍵保管メモリ２２に保管される。一方、上記共通鍵暗号方式にて暗号化されている使用条件とセキュリティＩＤを復号化する場合には、これらのデータを上記共通暗号復号回路２４に送ると共に、先に発生して共通鍵保管メモリ２２に保管しておいた前記共通鍵を読み出して同じく共通暗号復号回路２４に送る。当該共通暗号復号回路２４では、上記共通鍵を用いて上記使用条件とセキュリティＩＤを復号化する。このように復号化された使用条件は、ポイント使用情報格納メモリ２９に格納される。なお、ここで重要なのは、当該復号化されたコンテンツ鍵・使用条件は、当該プレーヤ１の外部、具体的には図２の集積回路１０内に設けられたコントローラ１６や共通鍵保管メモリ２２、ポイント使用情報格納メモリ２９から外部には取り出されないことである。

【０１１３】上記正当性の確認後、コントローラ１６は、ステップＳＴ７７のように、上記復号したコンテンツ鍵を上記コンテンツＩＤと共に上記共通鍵保管メモリ２２に格納させる。

【０１１４】その後、コントローラ１６は、ステップＳＴ７８にて、上記コンテンツ鍵を入手した旨を示すメッセージを作成し、このメッセージを前述同様に共通鍵暗号復号回路２４に送り、予め発生して共通鍵保管メモリ２２に保管しておいた前記共通鍵を読み出して同じく共通暗号復号回路２４に送る。当該共通暗号復号回路２４では、上記共通鍵を用いてメッセージを暗号化する。

【０１１５】当該メッセージの暗号化が終了すると、コントローラ１６は、ステップＳＴ７９のように、この暗号化されたメッセージを端子１２及び３を介してユーザ端末５０に送信する。この暗号化されたメッセージは、その後、管理センタ２１１に転送させる。

【０１１６】以上により、コンテンツ鍵・使用条件入手時のプレーヤ１における処理の流れが終了する。

【０１１７】次に、コンテンツ鍵・使用条件入手時のユーザ端末５０における処理の流れを、図１７を用いて説明する。

【０１１８】この図１７において、ユーザ端末５０は、ステップＳＴ８１にて、コンテンツ鍵・使用条件入手用のソフトウェアの立ち上げを行う。当該ソフトウェアが立ち上がると、このユーザ端末５０では、ステップＳＴ８２にて、上記ソフトウェアに従い当該ユーザ端末５０を操作するユーザに対して、希望のコンテンツの指定入力要求を行い、ユーザからコンテンツの指定がなされると、その指定情報を生成する。ユーザ端末５０は、上記ステップＳＴ８３にて、上記コンテンツの指定情報をプレーヤ１に対して送信する。

【０１１９】次に、ユーザ端末５０は、ステップＳＴ８４にて、前記図１６のステップＳＴ７４のように上記プレーヤ１にて作成されて転送されたデータを受信すると、ステップＳＴ８５にて、当該プレーヤ１から転送されたデータを、予めアドレスが登録されている管理センタ２１１へ転送する。

【０１２０】上記管理センタ２１１に対してデータの転送を行った後のユーザ端末５０は、管理センタ２１１からの返送を待ち、ステップＳＴ８６にて、管理センタ２１１から上記コンテンツＩＤで指定されたコンテンツ鍵・使用条件とセキュリティＩＤ等が暗号化されたデータの返送があると、ステップＳＴ８７にて当該管理センタ２１１からのデータをそのままプレーヤ１に転送する。

【０１２１】上記プレーヤ１に対してデータの転送を行った後のユーザ端末５０は、プレーヤ１からの返送を待ち、ステップＳＴ８８にて、プレーヤ１から前記図１６のステップＳＴ７９のように、上記コンテンツ鍵を入手した旨の暗号化されたメッセージの返送があると、ステップＳＴ８９にて当該ユーザ端末５０に接続されたディスプレイ装置に対して上記コンテンツ鍵入手が完了した旨の表示を行ってユーザに知らせる。

【０１２２】その後、上記プレーヤ１から返送された上記暗号化されたメッセージを、ステップＳＴ９０にて、管理センタ２１１に送付する。

【０１２３】以上により、コンテンツ鍵・使用条件入手時のユーザ端末５０における処理の流れが終了する。

【０１２４】次に、コンテンツ鍵・使用条件入手時の管理センタ２１１における処理の流れを、図１８を用いて説明する。

【０１２５】この図１８において、管理センタ２１１のユーザ端末との通信機能部１３３は、ステップＳＴ９１にて、前記図１６のステップＳＴ７４及び図１７のステップＳＴ８５のようにユーザ端末５０にてを介してプレーヤ１から送信されてきたコンテンツＩＤ，ユーザＩＤ、メッセージ、セキュリティＩＤの暗号化データを受信する。この受信したデータは、ユーザ管理機能ブロック１１０に送られる。

【０１２６】当該ユーザ管理機能ブロック１１０のコントロール機能部１１１は、上記受信した暗号化データに付加されたユーザＩＤに基づいて、当該暗号化を解くための共通鍵をデータベース部１１２から取り出し、通信文暗号・復号機能部１１４ではこの共通鍵を用いて上記暗号化データを復号する。また、コントロール機能部１１１は、データベース部１１２から読み出したユーザＩＤとセキュリティＩＤ発生機能部１１６からのセキュリティＩＤとを用いて、上記受信して復号化したデータの正当性を確認する。

【０１２７】なお、この時の共通鍵は、前記プレーヤ１から予め送られてきている前記セッション鍵であり、このセッション鍵は前述のように公開鍵暗号方式にて暗号化されて送られてきたものである。したがって、この暗号化されているセッション鍵の復号時には、前述同様に当該管理センタ２１１において、上記管理センタ２１１の公開鍵暗号方式の秘密鍵が取り出され、当該通信文暗号／復号機能部１１４にて上記暗号化されているセッション鍵が当該秘密鍵を用いて復号化される。このようにして得られたセッション鍵（共通鍵）が上記データベース部１１２に格納されている。

【０１２８】上記受信したデータの正当性を確認すると、コントロール機能部１１１は、コンテンツ管理機能ブロック１００に対して上記コンテンツＩＤにて指定されたコンテンツ鍵と使用条件を要求し、当該要求を受けたコンテンツ管理機能ブロック１００のコントロール機能部１０１は、上記コンテンツＩＤにて指定されたコンテンツ鍵と使用条件とをデータベース部１０２から読み出してユーザ管理機能ブロック１１０に転送する。コントロール機能部１１１は、ステップＳＴ９３に示すように、これらコンテンツ鍵と使用条件はセキュリティＩＤと共に通信文暗号／復号機能部１１４に送る。

【０１２９】ここで、コンテンツ鍵については前述した公開鍵暗号方式にて暗号化がなされ、使用条件及びセキュリティＩＤについては前述した共通鍵暗号方式にて暗号化がなされる。したがって、当該コンテンツ鍵を暗号化する時には、前記データベース部１１２からユーザ側２００の公開鍵（プレーヤ１に対応して予め格納されている公開鍵）が上記ユーザＩＤに基づいて取り出されて通信文暗号／復号機能部１１４に送られる。当該通信文暗号／復号機能部１１４では、上記公開鍵を用いて上記コンテンツ鍵を暗号化する。一方、上記使用条件及びセキュリティＩＤを暗号化する時には、上記データベース部１１２から上記ユーザＩＤで指定された共通鍵（セッション鍵）が取り出されて通信文暗号／復号機能部１１４に送られる。このときの通信文暗号／復号機能部１１４では、上記使用条件及びセキュリティＩＤを上記共通鍵を用いて暗号化する。

【０１３０】上記暗号化されたコンテンツ鍵と使用条件及びセキュリティＩＤは、管理機能ブロック１３０に送られ、ステップＳＴ９４のように、ユーザ端末との通信機能部１３３からユーザ端末５０に送信される。このユーザ端末５０に送信されたデータは、前記図１７のステップＳＴ８７及び図１６のステップＳＴ７５のようにユーザ端末５０を介してプレーヤ１に送付されることになる。

【０１３１】その後、管理センタ２１１は、前記図１６のステップＳＴ７９及び図１７のステップＳＴ９０のようにプレーヤ１にて生成されてユーザ端末５０を介して送信された暗号化メッセージの受信を待ち、ステップＳＴ９５のように上記通信機能部１３３が上記プレーヤ１が生成した暗号化メッセージを受信すると、当該管理センタ２１１は、ステップＳＴ９６のように、当該暗号化メッセージを共通鍵で復号化し、その復号メッセージから上記プレーヤ１がコンテンツ鍵と使用条件を入手したことを確認する。

【０１３２】以上により、コンテンツ鍵・使用条件入手時の管理センタ２１１における処理の流れが終了する。

【０１３３】上述した図１６から図１８の処理の流れにおけるプレーヤ１とユーザ端末５０と管理センタ２１１との間の情報送受のシーケンスは、図１９に示すように表すことができる。

【０１３４】すなわちこの図１９において、コンテンツ指定情報転送Ｔ２１では、前記図１７のステップＳＴ８３のように、ユーザ端末５０からプレーヤ１に対して、前記コンテンツ指定情報が転送される。作成データ転送Ｔ２２では、前記のステップＳＴ７４のように、プレーヤ１にて作成されたデータがユーザ端末５０に転送される。作成データ転送Ｔ２３では、当該ユーザ端末５０から上記プレーヤ１にて作成されたデータが管理センタ２１１に転送される。暗号化されたデータ送付Ｔ２４では、前記図１８のステップＳＴ９４のように、管理センタ２１１にて暗号化されたデータがユーザ端末５０に送付され、さらに、暗号化されたデータ送付Ｔ２５では、

当該暗号化されたデータがプレーヤ１に送付される。

【０１３５】メッセージ転送Ｔ２６では、前記図１６のステップＳＴ７９のように、コンテンツ鍵入手完了を示すメッセージを暗号化したデータがプレーヤ１からユーザ端末５０に転送され、さらに暗号化されたデータ送付Ｔ２７では、上記プレーヤ１からの暗号化されたメッセージが、ユーザ端末５０から管理センタ２１１に送付される。

【０１３６】次に、上述したようにしてポイント情報とディジタルコンテンツとコンテンツ鍵とを受け取ったプレーヤ１において、ユーザ端末５０を用いてディジタルコンテンツを実際に鑑賞する際の処理の流れについて、図２を参照しながら図２０を用いて説明する。

【０１３７】ここで、プレーヤ１の端子４には、前記ディジタルコンテンツが記憶された記憶メディアが接続されているとする。

【０１３８】この状態で、ステップＳＴ１０１のように、当該プレーヤ１に対して、ユーザ端末５０から鑑賞を希望するディジタルコンテンツが指定される。このとき、当該指定は、例えばユーザ端末５０をユーザが操作することによりなされる。

【０１３９】このとき、プレーヤ１のコントローラ１６は、ステップＳＴ１０２のように、上記ユーザ端末５０からのコンテンツ指定情報に応じて、上記記憶メディアに対するアクセスを行い、コンテンツのＩＤを読み取る。

【０１４０】上記コントローラ１６は、ステップＳＴ１０３のように、上記記憶メディアから読み取ったコンテンツＩＤに基づき、前記共通鍵保管メモリ２２に対してアクセスを行い、コンテンツ鍵が格納されているかどうかを確認すると共に、前記ポイント使用情報格納メモリ２９に対してアクセスを行い、使用条件が格納されているかどうかを確認する。

【０１４１】ここで、上記共通鍵保管メモリ２２やポイント使用情報格納メモリ２９内に、上記コンテンツ鍵と使用条件が格納されていないことを確認したとき、コントローラ１６は、ユーザ端末５０に対して当該コンテンツ鍵等が存在しない旨の情報を送り、これによりユーザ端末５０からは上記コンテンツ鍵等の入手を促すメッセージを前記ディスプレイ装置に表示する。この場合は、前述したコンテンツ鍵入手用のフローチャートのようにしてコンテンツ鍵等を入手する。このように、新たにコンテンツ鍵等を入手した場合には、ステップＳＴ１０４にて前述したように、その暗号化されているコンテンツ鍵等を復号化する。

【０１４２】次に、コントローラ１６は、ステップＳＴ１０５に示すように、上記復号化された使用条件を元に、ポイント情報格納メモリ２８に格納されているポイント情報の残高が足りているかどうかを確認する。上記ポイント情報格納メモリ２８に格納された上記ポイント情報の残高が足りないときには、コントローラ１６からユーザ端末５０に対して当該ポイント情報の残高が足りない旨の情報が送られ、これによりユーザ端末５０は、上記ポイント情報の入手を促すメッセージを前記ディスプレイ装置に表示する。この場合、前述したようなポイント情報入手用のフローチャートのようにしてポイント情報を入手する。

【０１４３】ここで、実際にディジタルコンテンツの鑑賞を行うとき、コントローラ１６は、ステップＳＴ１０６のように、当該鑑賞するディジタルコンテンツに応じて上記ポイント情報格納メモリ２８からポイント情報数を減額し、さらに当該ポイント情報の使用状態に応じた新たなポイント使用情報を、ポイント使用情報格納メモリ２９に格納する（ポイント使用情報の更新を行う）。このようにポイント使用情報格納メモリ２９に対して新たに格納されるポイント使用情報としては、上記鑑賞したディジタルコンテンツに対応する権利者情報（著作権者等）と減額されたポイント情報数の情報その他の情報などである。

【０１４４】その後、コントローラ１６は、ステップＳＴ１０７のように、これらポイント情報の減額やポイント使用情報の新たな格納等の課金用処理が完了したことを確認すると、記憶メディアからディジタルコンテンツを読み出す。

【０１４５】この記憶メディアから読み出されたディジタルコンテンツは暗号化されているため、コントローラ１６は、ステップＳＴ１０９のように、上記暗号化されたディジタルコンテンツを共通暗号復号回路２４に転送する。

【０１４６】この共通暗号復号回路２４では、ステップＳＴ１１０のように、コントローラ１６からの指示に基づいて、先に復号化して共通鍵保管メモリ２２に保管されているコンテンツ鍵を用いて、上記暗号化されているディジタルコンテンツの復号化を行う。

【０１４７】また、このディジタルコンテンツは前述したように所定の圧縮処理がなされているため、コントローラ１６は、ステップＳＴ１１１のように、上記暗号が復号化された上記圧縮処理されているディジタルコンテンツを、上記共通暗号復号回路２４から伸長回路２６に転送させ、ここで上記所定の圧縮処理に対応する伸長処理を行わせる。

【０１４８】その後、当該伸長されたディジタルコンテンツは、ステップＳＴ１１２のように、Ｄ／Ａ変換回路２７にてアナログ信号に変換され、ステップＳＴ１１３のように、集積回路１０の端子１３と当該プレーヤ１のアナログ出力端子２とを介して外部（例えばユーザ端末５０等）に出力される。

【０１４９】以上により、コンテンツ鑑賞時のプレーヤ１における処理の流れが終了し、ユーザはディジタルコンテンツの鑑賞が可能となる。

【０１５０】次に、上述したようなディジタルコンテンツの鑑賞に伴って前記プレーヤ１のポイント使用情報格納メディア２９に新たに格納されたポイント使用情報を、管理センタ２１１に返却する際の、プレーヤ１、ユーザ端末５０、管センタ３１０における処理の流れについて、図２と図３を参照しながら、図２１から図２４を用いて説明する。

【０１５１】図２１には、ポイント使用情報返却時のプレーヤ１における処理の流れを示している。

【０１５２】この図２１において、コントローラ１６は、ステップＳＴ１２１に示すように、ユーザ端末５０に予めインストールされているポイント使用情報返却用のソフトウェアの立ち上げが行われるまで待つ。

【０１５３】上記ユーザ端末５０の上記ポイント使用情報返却用のソフトウェアが立ち上がると、当該ソフトウェアに従ってユーザ端末５０に入力された情報が、ステップＳＴ１２２のように、前記ＰＣ用インターフェース端子３及び集積回路１０の端子１２を介して受信される。このときの上記ユーザ端末５０から供給される入力情報は、ユーザにより入力されるパスワード等である。

【０１５４】このコンテンツ指定情報を上記ユーザ端末５０から受信したコントローラ１６は、ステップＳＴ１２３にて、当該ユーザ端末５０から供給されたパスワードと、パスワード格納メモリ１４に格納されているパスワードとを比較して、当該パスワードが正しいどうかの確認をする。

【０１５５】上記パスワードの確認において正しいパスワードであると確認されたとき、コントローラ１６は、ステップＳＴ１２４のように、ポイント情報格納メモリ２８に格納されているポイント情報の残高と、ポイント使用情報格納メモリ２９に格納されているポイント使用情報とをそれぞれ読み出し、これら情報を暗号化する。

【０１５６】上記ポイント情報の残高とポイント使用情報の暗号化が終了すると、コントローラ１６は、ステップＳＴ１２５のように、ユーザＩＤ格納メモリ２３からユーザＩＤを読み出して上記暗号化したデータに添付する。

【０１５７】このユーザＩＤが添付されたデータは、ステップＳＴ１２６のように、コントローラ１６から端子１２及びＰＣ用インターフェース端子３を介してユーザ端末５０に転送される。このデータはその後管理センタ２１１に転送される。

【０１５８】なお、このときの暗号化にも前述したように共通鍵暗号方式が採用されている。すなわち、当該データの伝送に先立ち、前述同様に共通鍵の生成が行われ、この生成された共通鍵が前記公開鍵暗号方式にて暗号化（管理センタ２１１の公開鍵を用いた暗号化）され、ユーザＩＤと共に管理センタ２１１に送られている。

【０１５９】上述のようにしてユーザ端末５０にデータを転送した後、コントローラ１６は、上記管理センタ２１１から後述するデータがユーザ端末５０を介して転送されてくるのを待つ。

【０１６０】ここで、ステップＳＴ１２７のように上記管理センタ２１１からのデータを受信すると、プレーヤ１では、ステップＳＴ１２７のように、共通鍵暗号方式を使用して暗号化されている受信データを、前述同様に共通鍵を用いて復号化すると共にそのデータの正当性の確認を行う。すなわち、コントローラ１６は、上記復号化されたデータのセキュリティＩＤを、上記セキュリティＩＤ発生回路１９からのセキュリティＩＤとの比較によって確認することによる正当性の評価を行う。

【０１６１】また、上記管理センタ２１１から転送されてくるデータには、上記共通鍵を用いて暗号化された処理完了のメッセージも含まれている。したがって、上記セキュリティＩＤの確認が終了した後のコントローラ１６は、上記暗号化された処理完了メッセージを共通暗号復号回路２４に送り、ここで共通鍵を用いた復号化を行わせ、この復号化した処理完了メッセージを受け取ることで、上記管理センタ２１１での処理が完了したことを確認する。

【０１６２】以上により、ポイント使用情報返却時のプレーヤ１における処理の流れが終了する。

【０１６３】次に、ポイント使用情報返却時のユーザ端末５０における処理の流れを、図２２を用いて説明する。

【０１６４】この図２２において、ユーザ端末５０は、ステップＳＴ１３１にて、ポイント使用情報返却用のソフトウェアの立ち上げを行う。当該ソフトウェアが立ち上がると、このユーザ端末５０では、ステップＳＴ１３２にて、上記ソフトウェアに従い当該ユーザ端末５０を操作するユーザに対して、パスワード等の入力要求を行い、ユーザからパスワードの入力がなされると、そのパスワードをプレーヤ１に転送する。

【０１６５】次に、ユーザ端末５０は、ステップＳＴ１３３にて、前記図２１のステップＳＴ１２６のように上記プレーヤ１にて作成されて転送されたデータを受信すると、ステップＳＴ１３４にて、当該プレーヤ１から転送されたデータを、予めアドレスが登録されている管理センタ２１１へ転送する。

【０１６６】上記管理センタ２１１に対してデータの転送を行った後のユーザ端末５０は、管理センタ２１１からの返送を待ち、ステップＳＴ１３５にて、管理センタ２１１からプレーヤ１に対して送られるデータを受信すると、当該データをそのままプレーヤ１に転送する。

【０１６７】上記プレーヤ１に対してデータの転送を行った後のユーザ端末５０は、処理が完了した旨をユーザに知らしめるための表示をディスプレイ装置に行い、ユーザからの確認を受ける。

【０１６８】以上により、ポイント使用情報返却時のユ

ーザ端末５０における処理の流れが終了する。

【０１６９】次に、ポイント使用情報返却時の管理センタ２１１における処理の流れを、図２３を用いて説明する。

【０１７０】管理センタ２１１のユーザ端末との通信機能部１３３において、ステップＳＴ１４１のように、前記図２１のステップＳＴ１２６及び図２２のステップＳＴ１３４によって前記ユーザ端末５０を介してプレーヤ１から送信されてきたポイント使用情報等のデータを受信する。

【０１７１】このデータを受信すると、管理センタ２１１のユーザ管理機能ブロック１１０は、ステップＳＴ１４２のように、コントロール機能部１１１の制御の元で、当該受信したデータに添付されたユーザＩＤに基づいて、データベース部１１２から前述同様に予め受け取って格納している共通鍵を入手すると共にセキュリティＩＤを入手する。

【０１７２】上記データベース部１１２から上記ユーザＩＤに対応する共通鍵とセキュリティＩＤを入手すると、ステップＳＴ１４３に示すように、管理センタ２１１のユーザ管理機能ブロック１１０の通信文暗号／復号機能部１１４において、上記共通鍵を用いて、上記プレーヤ１からの上記暗号化されたポイント使用情報等のデータの復号化を行い、さらにコントロール機能部１１１において、当該復号化したデータ中のセキュリティＩＤと上記データベース部１１２から読み出したセキュリティＩＤとの比較によって、アクセスしてきたユーザ側２００（プレーヤ１）が正当な使用者であるかどうかの内容確認を行う。

【０１７３】上記正当性と内容の確認後のデータは、使用情報管理機能ブロック１２０に転送される。この使用情報管理機能ブロック１２０のコントロール機能部１２１は、ステップＳＴ１４４に示すように、上記プレーヤ１から送られてきたポイント情報の残高とポイント使用情報とを用い、データベース部１２２に格納されている情報を用いて上記ユーザ側２００の使用に不正がないかどうかの確認を行う。同時に、当該不正なきことを確認した場合には、使用情報演算機能部１２３においてポイント情報の残高とポイント使用情報をまとめる演算を行う。

【０１７４】その後、ステップＳＴ１４５に示すように、ユーザ管理機能ブロック１１０のコントロール機能部１１１は、セキュリティＩＤ発生機能部１１６を制御してセキュリティＩＤを算出させ、さらに確認メッセージ発生機能部１１５を制御して処理完了のメッセージを生成させる。これらセキュリティＩＤと処理完了メッセージは、ユーザ管理機能ブロック１１０の通信文暗号／復号機能部１１４にて前記共通鍵を用いて暗号化される。

【０１７５】上記暗号化されて生成されたデータは、ステップＳＴ１４６に示すように、ユーザ端末との通信機能部１３３からユーザ端末５０に送られ、前記図２２のステップＳＴ１３５と図２１のステップＳＴ１２７のように当該ユーザ端末５０からプレーヤ１に転送されることとなる。

【０１７６】以上により、ポイント使用情報返却時の管理センタ２１１における処理の流れが終了する。

【０１７７】上述した図２１から図２３の処理の流れにおけるプレーヤ１とユーザ端末５０と管理センタ２１１との間の情報送受のシーケンスは、図２４に示すように表すことができる。

【０１７８】すなわちこの図２４において、入力情報転送Ｔ３１では、前記図２２のステップＳＴ１３２のように、ユーザ端末５０からプレーヤ１に対して、前記パスワード等の入力情報が転送される。作成データ転送Ｔ３２では、前記図２１のステップＳＴ１２６のように、プレーヤ１が作成したデータがユーザ端末５０に転送される。作成データ転送Ｔ３３では、前記図２２のステップＳＴ１３４のように、上記プレーヤ１にて作成されたデータが上記ユーザ端末５０から管理センタ２１１に転送される。データ転送Ｔ３４では、前記図２３のステップＳＴ１４６のように、管理センタ２１１にて作成されたデータが、ユーザ端末５０に転送される。データ転送Ｔ３５では、前記図２１のステップＳＴ１２７のように、管理センタ２１１にて作成されたデータがユーザ端末５０を介してプレーヤ１に転送される。

【０１７９】本実施の形態のシステムのプレーヤ１とユーザ端末５０と管理センタ２１１の実際の動作は、上述したような流れとなる。

【０１８０】ここまでは、本実施の形態のシステムにおける全体の処理の流れを説明してきたが、これ以降は、本実施の形態のシステムの主要部の個々の動作を詳細に説明する。

【０１８１】先ず、本発明実施の形態における暗号化及び圧縮と、伸長及び復号化の動作についての説明を行う。

【０１８２】上述した実施の形態のシステムのように、ネットワークを使ってディジタルコンテンツを配信する際には、そのデータ量を抑えるために圧縮／伸長技術を使用し、コピー防止或いは課金のために暗号化／圧縮技術が使われる。すなわち、配信側（上述の例では管理センタ２１１側）でディジタルコンテンツを圧縮し、さらに暗号化処理することが行われる。上述の例のように送信側（管理センタ２１１側）にて生成されたディジタルコンテンツ（暗号化／圧縮データ）をネットワークを使って配信するとき、受信側（上述の例ではプレーヤ１）では上記暗号化及び圧縮されたディジタルコンテンツを受信後に復号化し、さらに伸長してディジタルコンテンツを復元することが行われる。なお、上記暗号化と圧縮、復号化と伸長の処理の順番は入れ替わる場合もあ

る。

【０１８３】上記ディジタルコンテンツに著作権等が存在する場合、上記受信側は、上記ディジタルコンテンツを上記復号化と伸長する際に、上記著作権者等の意思に従い、課金されることになる。この課金は、主として復号化の鍵すなわちコンテンツ鍵を購入することにより行われるが、このコンテンツ鍵を購入する方法には種々ある。

【０１８４】ここで、上述したように、ディジタルコンテンツを圧縮して暗号化し、復号化して伸長するような処理手順に従った場合、例えば悪意を持ったユーザは上記復号化済みの圧縮データを比較的簡単に入手することができることになる。すなわちディジタルコンテンツの圧縮データは、一般に容量が大きく、したがって例えば受信側の一般的なコンテンツ再生装置の内部メモリではなく、安価が外部メモリに蓄積される場合が多いため、この外部メモリから直接、或いは外部メモリとの接続部分で上記圧縮されたディジタルコンテンツを不正に取り出すことが容易だからである。

【０１８５】また、圧縮に対する伸長方式のアルゴリズムは公開されている場合が多く、また伸長方式のアルゴリズムには一般的な暗号の鍵のようにそれぞれ隠しておけば処理できないようなものも存在していない。しかも、上記復号化された圧縮ディジタルコンテンツは、上記送信側から配信された暗号化と圧縮とがなされたディジタルコンテンツと比較して、データ量的に変わらず、したがって、上記復号化された圧縮ディジタルコンテンツを悪意を持って配信するののも容易である。すなわち、上記圧縮した後に暗号化されてディジタルコンテンツを配信する方式によると、誰でも容易に伸長できる圧縮ディジタルコンテンツが、悪意を持ったユーザに容易に盗難され、このため著作権者等の意思の届かないところでさらに配信されたり、伸長されたりする危険性が大きい。

【０１８６】そこで、本発明の実施の形態では、このような状況に鑑み、ネットワークを使って配信するディジタルコンテンツの安全性を向上させることを可能にするため、上記図２のプレーヤ１において、以下の図２５のフローチャートに示すような処理を行っている。

【０１８７】すなわち図２のプレーヤ１の共通暗号復号回路２４における復号化処理と上記伸長回路２６における伸長処理では、前記記憶メディアから読み出された暗号化と圧縮処理されたディジタルコンテンツのデータを、ステップＳＴ１５１のように、先ず、復号化処理のアルゴリズムの処理単位Ｘビットと、伸長処理のアルゴリズム処理単位Ｙビットとの最小公倍数１ｃｍ（Ｘ，Ｙ）の単位に分割する。

【０１８８】次に、上記最小公倍数１ｃｍ（Ｘ，Ｙ）の単位に分割された上記暗号化と圧縮処理がなされているディジタルコンテンツのデータは、ステップＳＴ１５２に示すように、当該最小公倍数１ｃｍ（Ｘ，Ｙ）の単位毎に、上記共通暗号復号回路２４にて復号化処理が行われる。

【０１８９】当該復号化処理により得られた最小公倍数１ｃｍ（Ｘ，Ｙ）の単位の圧縮されているディジタルコンテンツのデータは、ステップＳＴ１５４に示すように、当該単位分の全ての圧縮データに対して上記伸長回路２６にて伸長処理が行われる。

【０１９０】その後、この最小公倍数１ｃｍ（Ｘ，Ｙ）の単位毎の復号化及び伸長処理は、上記暗号化と圧縮処理されたディジタルコンテンツの全データについての処理が終了するまで続けられる。すなわち、ステップＳＴ１５５に示すように、最小公倍数１ｃｍ（Ｘ，Ｙ）の単位毎の復号化及び伸長処理がディジタルコンテンツの全データに対して完了したか否かの判断がなされ、完了していない時にはステップＳＴ１５２に戻り、完了したときに当該処理のフローチャートが終了する。

【０１９１】これにより全データの復号化及び伸長されたディジタルコンテンツが得られることになる。

【０１９２】なお、当該プレーヤ１における図２５のフローチャートの処理でも、上記最小公倍数１ｃｍ（Ｘ，Ｙ）単位の復号化データは存在することになるが、当該復号化データのデータ量は少ない。このため、比較的高価でも安全性の高い内部メモリに保存することができるようになり、したがって前述したような外部メモリに保存する場合のように盗まれる可能性は非常に低いものとなる。

【０１９３】また、本実施の形態における上記プレーヤ１では、上記安全性を確保するための内部メモリとして、図２のバッファメモリ２５が上記共通暗号復号回路２４と伸長回路２６との間に設けられている。すなわちこのバッファメモリ２５は、１チップの集積回路１０内に設けられており、外部からアクセスされ難く、したがってデータが外部に取り出されることはない。

【０１９４】上述のフローチャートでは、最小公倍数１ｃｍ（Ｘ，Ｙ）の単位分の全てのデータに対して復号化及び伸長処理を行うようにしており、このための具体的構成としては、例えば図２６に示す構成のように、最初に復号化処理のアルゴリズムの処理単位Ｘビットにディジタルコンテンツのデータを分割し、このＸビットのデータに復号化処理を施し、その後当該復号化処理されたＸビットの圧縮されているデータを、伸長処理のアルゴリズム処理単位Ｙビット分まとめ、当該Ｙビットの圧縮データを伸長することで、上述のように最小公倍数１ｃｍ（Ｘ，Ｙ）の単位での復号化及び伸長処理を実現するようにしている。

【０１９５】このことを実現するプレーヤ１の共通暗号復号回路２４は、入力部３０と暗号復号部３１とからなり、上記伸長回路２６は、伸長部３２と出力部３３とからなる。これら共通暗号復号回路２４と伸長回路２６の

間に前記バッファメモリ２５が設けられている。

【０１９６】ここで、より具体的な例として、上記ディジタルコンテンツに対する暗号化処理が例えばＤＥＳ（Data Encription Standard）暗号を用いて行われているのであれば、当該暗号化処理とそれに対応する復号化処理は、６４ビット単位で行われることになる。

【０１９７】また、圧縮されたディジタルコンテンツに対する伸長処理の場合、その圧縮率やサンプリング周波数によっても異なるが、現状では１Ｋ～２Ｋビット／チャンネル単位で処理される場合が多い。ここでは、便宜的に１．２８Ｋビット毎に処理されると仮定する。

【０１９８】したがって、上記ＤＥＳ暗号化方式と上記１．２８Ｋビット毎の圧縮伸長方式を用いたシステムの場合、上記最小公倍数１ｃｍは１．２８Ｋとなる。

【０１９９】このような条件のもと、図２６の共通暗号復号回路２４の入力部３０には、前記暗号化されて圧縮されたディジタルコンテンツが入力される。当該入力部３１では、上記暗号化されて圧縮されたディジタルコンテンツを、上記復号化処理のアルゴリズムの処理単位Ｘビット、すなわち６４ビットづつのデータに分割して暗号復号部３１に出力する。

【０２００】この暗号復号部３２では、上記Ｘビットすなわち６４ビットのデータを、当該６４ビット毎に復号化処理する。この６４ビット毎の復号化により得られた６４ビットの圧縮されているデータは、バッファメモリ２５に送られる。

【０２０１】当該バッファメモリ２５は、前記コントローラ１６からの指示に従い、伸長処理のアルゴリズム処理単位Ｙビット、すなわち１．２８Ｋビット分の圧縮データがたまった時点で、当該１．２８Ｋビット分の圧縮データを一括して出力し、この圧縮データが上記伸長回路２６の伸長部３２に送られる。

【０２０２】上記伸長部２６は、上記入力された１．２８Ｋビット分の圧縮データを伸長して出力部３３に出力する。

【０２０３】また、コントローラ１６は、バッファメモリ２５にたまったデータ量をモニタしながら、復号化部３１の処理と伸長部３２の処理をコントロールする。

【０２０４】なお、このケースであれば、復号化処理を２０個（＝１２８０／６４）並列で処理すれば、より高速な処理システムになる。

【０２０５】その他、前記図２や図２６のようなハードウェア構成ではなく、プログラマブルデバイスにて上述した処理を行う場合には、バッファメモリ２５の状況に応じて、例えばコントローラ１６が復号化プログラム或いは伸長プログラムに基づいて処理を行うことになる。

【０２０６】上述の説明では、圧縮した後に暗号化したディジタルコンテンツがプレーヤ１に供給され、プレーヤ１ではこの圧縮及び暗号化されたディジタルコンテンツを復号化した後に伸長する例を挙げたが、暗号化した後に圧縮されたディジタルコンテンツを伸長して復号化する場合であっても、上述同様の効果を得ることができる。

【０２０７】また、本発明は、圧縮／伸長並びに暗号化／復号化のアルゴリズムが限定されることはなく、いかなる方式に対しても有効である。

【０２０８】このように、本発明によれば、ネットワークを使って配信するディジタルコンテンツの安全性が向上する。

【０２０９】次に、前記セキュリティＩＤの発生動作についての説明を行う。

【０２１０】本実施の形態のように、ポイント情報を予め入手しておき、ディジタルコンテンツの鑑賞に応じて当該ポイント情報を減額するような方式の場合、前述したように、ネットワーク上の管理センタ２１１は、ユーザ側２００のユーザ端末５０からのポイント情報の購入依頼の通信を受けた後に、金融機関２２０その他と任意の確認を行った後、そのポイント情報を暗号化して、ユーザ側２００のプレーヤ１にネットワーク経由で送る。

【０２１１】本実施の形態のように、ポイント情報を予め入手しておき、ディジタルコンテンツの鑑賞に応じて当該ポイント情報を減額するような方式の場合、管理センタ２１１とプレーヤ１（ユーザ端末５０）との間で、ポイント情報の購入の度に、毎回同じようなデータのやり取りを行う（例えば暗号化された「３０００円分のポイント情報の補充要求」及びそれに対応した「３０００円分のポイント情報」といった情報のやりとりを行う）と、例えば悪意を持つ者によると、金融機関２２０へのいわゆる「成り済まし」による金額補充が問題点となる。なお、ここに言う金融機関への「成り済まし」とは、上記悪意を持った者が本来のユーザ（本実施の形態ではユーザ側２００）に成り済まして、不正にポイント情報を入手するようなことを言う。

【０２１２】すなわち、ポイント情報の購入の度に毎回同じようなデータのやり取りを行っていると、例えば悪意を持った者が当該データを通信回線から盗み出して同じデータを生成し、管理センタ２１１に対して送り先を自分（悪意を持った者）にしてポイント情報の入手を依頼したような場合、当該悪意を持った者がポイント情報を入手できることになり、さらにこのポイント情報の購入代金の請求は本来のユーザ側２００になされることになるという問題が発生するおそれがある。

【０２１３】そこで、こういった不正を防止するために、本発明実施の形態のシステムでは、予め受信側（プレーヤ１側）と配信側（管理センタ２１１側）の両者で連動している乱数発生機能により発生させられた乱数を安全性向上のために使用している。本実施の形態では、上記乱数として前記セキュリティＩＤを発生している。なお、両者間で乱数発生を連動させるには、例えばユーザの登録手続きなどの際に、例えばタイマ１８を初期化

するなどして、両者間の動作を同期させれば良い。

【０２１４】すなわち、この乱数（セキュリティＩＤ）を用いた場合の管理センタ２１１からプレーヤ１への例えばポイント情報入手時の動作は、以下のような流れとなる。

【０２１５】ポイント情報の購入時、管理センタ２１１からプレーヤ１に対して送られるデータは、前述したように例えばプレーヤ１から予め入手した共通鍵（セッション鍵）を用いて暗号化されたポイント情報と上記発生されたセキュリティＩＤからなるデータとなされる。

【０２１６】プレーヤ１のコントローラ１６は、当該管理センタ２１１から受け取ったデータを前述したように共通暗号復号回路２４に送り、ここで前記共通鍵を用いて復号化処理を行う。これにより、管理センタ２１１から送られてきたポイント情報とセキュリティＩＤとが得られることになる。

【０２１７】その後、プレーヤ１のコントローラ１６は、上記管理センタ２１１から送られてきたセキュリティＩＤと、自身のセキュリティＩＤ発生回路１９にて発生したセキュリティＩＤとを比較する。この比較において、コントローラ１６は、管理センタ２１１からのセキュリティＩＤと、上記自身が発生したセキュリティＩＤとが一致したときのみ、上記管理センタ２１１から送られてきたポイント情報を、前記ポイント情報格納メモリ２８に格納する。

【０２１８】これにより、正当なユーザ側２００のプレーヤ１のみがポイント情報を入手できることになる。言い換えれば、正当なユーザ側２００のプレーヤ１と同じようなプレーヤを持っている悪意の者が、前記成り済ましによって不正にポイント情報を入手しようとしても、当該悪意の者が持っているプレーヤのセキュリティＩＤと上記管理センタ２１１から送られてきたセキュリティＩＤとは一致しないため、この悪意を持った者は前記成り済ましによる不正なポイント情報入手ができないことになる。

【０２１９】勿論、ユーザ側２００のプレーヤ１で発生するセキュリティＩＤは、当該プレーヤ１の集積回路１０内に設けられたセキュリティＩＤ発生回路１９によって発生されるものであり、外部には取り出せないものであるため、悪意を持った者が当該セキュリティＩＤを盗むことはできない。

【０２２０】上記セキュリティＩＤとしての乱数を発生する構成には種々のものがあるが、その一例を図２７に示す。この図２７の構成は、前記図２のセキュリティＩＤ発生回路１９の一具体例である。

【０２２１】この図２７において、一方向関数発生部４０は、いわゆる一方向性関数を発生する。なお、上記一方向性関数とは、比較的計算が簡単な関数で逆関数がはるかに計算が困難なものである。この一方向関数は、予め秘密通信等で受け取って当該一方向関数発生部４０に保存しておくことも可能である。なお、一方向関数発生部４０は、前記図２の集積回路１０内に設けられたタイマ１８からの時間情報を入力関数として上記一方向関数を発生するようにすることも可能である。上記一方向関数は、乱数決定部４３に送られる。

【０２２２】また、ユーザ定数発生部４１は、ユーザ毎に定められた所定のユーザ定数を発生する。このユーザ定数は、予め秘密通信等で送付されて当該ユーザ定数発生部４１に保存されるものである。なお、このユーザ定数は、例えば前記ユーザＩＤ格納メモリ２３が格納するユーザＩＤを用いることもできる。

【０２２３】乱数データベース４２は、乱数を格納するものであり、例えば９９個の乱数を格納している。

【０２２４】通信回数記憶部４４は、例えばコントローラ１６から送られてくる通信回数情報を記憶するものである。この通信回数情報とは、プレーヤ１と管理センタ２１１との間の通信回数を示す情報である。

【０２２５】これら一方向関数とユーザ定数と通信回数情報は、乱数決定部４３に送られる。当該乱数決定部４３は、例えば前記タイマ１８からの時間情報に基づき、上記一方向関数とユーザ定数から、予め乱数データベース部４２に記憶された範囲の乱数を発生させる（例えば９９個）。

【０２２６】すなわち、この乱数決定部４３では、上記通信回数情報が例えば１回目の通信であれば、９９個目の乱数を上記乱数データベース部４２から取り出し、また例えば通信回数情報がｎ回目の通信であれば１００－ｎ個目の乱数を上記乱数データベース４２から取り出し、この取り出した乱数を前記セキュリティＩＤとして出力する。

【０２２７】このセキュリティＩＤ発生の構成は、プレーヤ１と管理センタ２１１とで同じものを有している。

【０２２８】なお、乱数データベース部４２に格納している全ての乱数を使い終わったときには、上記乱数決定部４２において１００個～１９９個目の乱数を計算するか、或いは新たな乱数や１方向性関数を秘密通信するなどして、乱数データベース部４２に再格納したり、一方向性関数発生部４０に再構築する。

【０２２９】また、上述した説明では、乱数（セキュリティＩＤ）を発生させて通信毎の安全性を高めるようにしているが、本実施の形態では、前述のようにユーザ側２００と管理センタ２１１側との間で通信を行う毎に、毎回異なる共通鍵（セッション鍵）をプログラマブルに発生させるようにもしているので、さらに安全性が高められている。

【０２３０】ここで、実際に送信される送信文（例えばメッセージ等）について上記乱数が挿入されると共に、セッション鍵による暗号化がなされる様子と、受信文から乱数が取り出されて正当性の確認がなされる様子を図２８と図２９を用いて説明する。なお、これら図２８、

図２９の例では、送信文に署名（ディジタル署名）を付加するようにもしている。

【０２３１】この図２８において、先ず、前記共通鍵を公開鍵暗号方式にて暗号化して送信する流れとして、通信用共通鍵発生工程Ｐ７では前記セッション鍵を通信用に用いる共通鍵として発生し、この共通鍵は公開鍵暗号化工程Ｐ８にて受信側の公開鍵で暗号化される。この暗号化された共通鍵は、受信側に送られる。

【０２３２】一方、送信文としてのメッセージを共通鍵暗号方式にて暗号化して送信する場合の流れとして、例えばメッセージ生成行程Ｐ１ではメッセージＭが生成されると共に、乱数発生工程Ｐ５にて乱数（前記セキュリティＩＤ）が発生される。これらメッセージＭと乱数は、共通鍵暗号化工程Ｐ６に送られる。この共通鍵暗号化工程Ｐ６では、上記通信用共通鍵発生工程Ｐ７にて発生した共通鍵を用いて、上記メッセージＭと乱数を暗号化する。

【０２３３】さらに、上記ディジタル署名を付加する場合、上記メッセージＭはハッシュ値計算工程Ｐ２に送られる。当該ハッシュ値計算工程Ｐ２では、上記メッセージＭからいわゆるハッシュ値が計算される。なお、ハッシュ値とはハッシュ法にて求められるアドレス情報であり、ハッシュ法とはデータ（この場合はメッセージＭ）の内容の一部（キーワード）に所定の演算を施し、その結果をアドレスとして使用するものである。このメッセージから生成されたハッシュ値（Ｍ）はディジタル署名として、秘密鍵暗号化工程Ｐ４に送られる。この秘密鍵暗号化工程Ｐ４では、送信側の秘密鍵で上記ディジタル署名を暗号化する。この暗号化されたディジタル署名は、共通鍵暗号化工程Ｐ６に送られる。これにより共通鍵暗号化工程Ｐ６では、上記通信用共通鍵発生工程Ｐ７にて発生した共通鍵を用いて、上記ディジタル署名を暗号化する。

【０２３４】これらメッセージＭとディジタル署名と乱数が受信側に送信される。

【０２３５】次に、図２９を用いて、図２８に対応する受信側での処理の流れを説明する。

【０２３６】この図２９において、先ず、前記共通鍵を公開鍵暗号方式にて復号化する流れとして、秘密鍵復号化工程Ｐ１１では、上記送信側から送信されてきた共通鍵を当該受信側の秘密鍵で復号化する。

【０２３７】一方、前記共通鍵暗号方式にて暗号化されたメッセージＭを復号化する流れとして、共通鍵復号工程１３では、上記送信されてきたメッセージＭを上記秘密鍵復号化工程Ｐ１１にて復号化した共通鍵を用いて復号化する。この復号化されたメッセージＭは、他機能送信工程Ｐ２０にて他の工程に送られることになる。

【０２３８】また、ディジタル署名を復号する流れでは、上記共通鍵復号化工程Ｐ１３にて復号化されたハッシュ値が、公開鍵復号化工程Ｐ１４にて送信側の公開鍵を用いて復号化される。同時に、ハッシュ値計算工程Ｐ1.7では、上記メッセージＭからハッシュ値を計算する。これら公開鍵復号化工程Ｐ１４により復号されたハッシュ値と上記ハッシュ値計算工程Ｐ１７にて計算されたハッシュ値とは、比較工程Ｐ１９にて比較され、改竄されていないことの確認が行われる。

【０２３９】さらに、送信された乱数については、上記共通鍵復号化工程Ｐ１３にて復号化された乱数と、当該受信側の乱数発生工程Ｐ２１にて発生された乱数とが、正当正確認工程Ｐ２２にて比較され、正当性の確認が行われる。

【０２４０】ところで、前述した図１に示した本実施の形態のシステムでは、ユーザ側２００に対するシステム側として、システム管理会社２１０と仮想店舗２３０とコンテンツプロバイダ２４０とが設けられている。なお、図１の金融機関２２０は、例えば外部の銀行等である。

【０２４１】上記システム管理会社２１０の管理センタ２１０は、仮想店舗２３０におけるディジタルコンテンツの展示や配信の管理、金融機関２２０との間でユーザ側２００の課金情報や各種情報の収集、分配及びそれらの管理、コンテンツプロバイダ２４０からのディジタルコンテンツの暗号化、扱う情報のセキュリティ管理など、システム側の主要な作業のほぼ全てを行っている。

【０２４２】しかし、上述したようなネットワークを使ってディジタルコンテンツを配信するシステムにおいて、ユーザ側がシステム側からディジタルコンテンツを入手する際や、ディジタルコンテンツの使用に伴う課金の際には、システム側に通信が集中することになり、ユーザ側に対して満足のいくレスポンスが得られなくなるおそれがある。

【０２４３】そこで、本発明の他の実施の形態では、システム管理会社２１０の機能、より具体的には管理センタ２１１の機能を、以下のように分割することで、上述したような通信の集中を防ぎ、通信のレスポンスを向上させることを可能にしている。

【０２４４】すなわち、本発明の他の実施の形態では、図３０に示すように、ユーザ側２００に対するシステム側の構成を、ディジタルコンテンツを展示，配信する機能を有するコンテンツ展示配信機関３１０と、一定の地域のユーザの課金情報を管理する機能を有する課金情報管理機関３２０と、ディジタルコンテンツを暗号化する等のデータ生成と上記コンテンツ展示配信機関３１０への生成データの配信と上記課金情報管理機関３２０からの情報収集と収益分配とシステム全体のセキュリティ管理その他を行う機能を有するシステム管理機関３３０とに分割し、各機関３１０，３２０，３３０がそれぞれ独立にユーザ側２００と通信可能になされている。

【０２４５】この図３０のような構成において、コンテンツ展示配信機関３１０は、世界中のネットワーク上に

散らばって複数配置可能なものであり、ユーザ側２００は通信費さえ支払えばどの地域のコンテンツ展示配信機関３１０へでもアクセスできる。例えばユーザ側２００がディジタルコンテンツを入手したい場合には、ユーザ側２００から上記コンテンツ展示配信機関３１０にアクセスして、ディジタルコンテンツを入手する。このときのディジタルコンテンツは、システム管理機関３３０によって暗号化等されたディジタルコンテンツ、すなわちユーザ側２００にネットワークを使って直接送信可能な状態になされたものである。

【０２４６】また、課金情報管理機関３２０は、課金情報を扱うため、余り多くのユーザを抱え込むことは安全性管理上好ましくなく、したがって、適度な数のユーザ毎に設置する。但し、あまり多く設置すると、悪意を持った第３者からの攻撃ポイント（課金情報管理機関３２０）を増やすことになり、トレードオフになるので、最適化することが望ましい。例えばユーザ側２００が課金に関する通信を行う場合には、ユーザ側２００から上記課金情報管理機関３２０に対してアクセスする。

【０２４７】上記システム管理機関３３０は、ユーザのシステムへの加入や決済方法の登録、ユーザからの集金や前記権利者，コンテンツ展示配信機関３１０，課金情報管理機関３２０等の利益受益者への利益配付など、セキュリティ上重要な情報の管理をまとめて行うことで、セキュリティを向上させる。但し、当該システム管理機関３３０は世界に１箇所のみ設けるわけではなく、あるまとまった単位、例えば国などの単位で設置するのが望ましい。例えば、ユーザ側２００がこのシステムへの加入や決済方法の登録などセキュリティ上重要な通信を行う場合には、ユーザ側２００から上記システム管理機関３３０に対してアクセスして行う。当該ユーザからの集金と利益受益者への利益配付は上記課金情報管理機関３２０から情報を入手した当該システム管理機関３３０がまとめて行う。また、著作権者等が有するソースデータすなわちコンテンツは、当該システム管理機関３３０に供給され、ここで暗号化等がなされたディジタルコンテンツに変換され、上記コンテンツ展示配信機関３１０に配信される。

【０２４８】上述のように、システム側の機能を例えば３つの機関３１０，３２０，３３０に振り分け、ユーザ側２００と各機関３１０，３２０，３３０との間で直接アクセス可能とすることにより、通信の集中を防ぎ、通信のレスポンスを向上させることが可能となる。また、コンテンツ展示配信機関３１０によれば、既存のいわゆるバーチャルモールのようなものにも対応でき、販売促進にも有効であり、ユーザにとって魅力のあるものになる。課金情報管理機関３２０を別に分けることにより、コンテンツの展示や販売機能と結託した不正防止に役立つ。また、管理するユーザを一定の数に抑えられるため、不正に対する管理機能もより効果的である。

【０２４９】以下に、上述した図３０に示した本発明の他の実施の形態のシステムにおいて、ユーザのシステムへの加入、ポイント情報の購入や暗号化されたディジタルコンテンツの復号用のコンテンツ鍵等の入手時の情報の流れ、コンテンツとコンテンツ鑑賞用の情報の流通の際の流れ、コンテンツの使用に伴う課金情報の流れについて説明する。

【０２５０】先ず、図３１を用いて、ユーザのシステムへの加入時の流れの主要部を説明する。

【０２５１】ユーザのシステムへの加入登録の際には、システム管理機関３３０のユーザ加入サポート機能ブロック４０２による以下の手順の従って登録作業が行われる。

【０２５２】ユーザ側２００すなわち前記プレーヤ１及びユーザ端末５０からは、先ず加入意思送付Ｔ４１のようにシステムへの加入の意思を示す情報が、システム管理機関３３０に対してネットワークを介して送付される。システム管理機関３３０の通信機能ブロック４０１に入力された上記加入意思の情報は、ユーザ加入サポート機能ブロック４０２に送られる。

【０２５３】当該ユーザ加入サポート機能ブロック４０２は、上記加入意思情報を受信すると、加入必要ファイル送付Ｔ４２のように、加入に必要なファイルの情報を通信機能ブロック４０１を介してユーザ側２００に送られる。

【０２５４】ユーザ側２００では、上記システム管理機関３３０から送られてきた加入必要ファイルに基づいて、所定のフォーマットに従った加入申請書の作成が行われる。当該作成された加入申請書は、加入申請書送付Ｔ４３のように、システム管理機関３３０に送付される。

【０２５５】上記加入申請書を受け取ったユーザ加入サポート機能ブロック４０２は、クライアント機能送付Ｔ４４のように、クライアントの機能を解説する情報を、ユーザ側２００に送付する。

【０２５６】当該クライアント機能の情報を受け取ったユーザ側２００からは、ユーザ情報送付Ｔ４５のように、ユーザ側の情報、例えば前述したような口座番号やクレジット番号，名前や連絡先等のユーザ情報を、システム管理機関３３０に送付する。

【０２５７】当該ユーザ情報の送付を受けたユーザ加入サポート機能ブロック４０２は、登録手続き完了通知Ｔ４６のように、加入の登録手続きが完了した旨の情報を、ユーザ側２００に通知する。

【０２５８】また、このユーザ加入登録の手続き完了後、システム管理機関３３０のユーザ加入サポート機能ブロック４０２は、ユーザ情報送付Ｔ４７のように、通信機能ブロック４０１を介して、課金情報管理機関３２０に対してユーザ情報を転送する。このユーザ情報を受け取った課金情報管理機関３２０は、当該ユーザ情報を

データベース機能ブロック３６７に保存する。

【０２５９】以上により、ユーザのシステムへの加入時の主な流れが終了する。なお、この図３１に挙げられている他の構成についての説明は後述する。

【０２６０】次に、図３２を用いて、ポイント情報の購入や暗号化されたディジタルコンテンツの復号用の鍵等の入手時の情報の流れの主要部を説明する。なお、上記ポイント情報の購入や暗号化されたディジタルコンテンツの復号用のコンテンツ鍵の情報は、コンテンツを使用するための情報であるので、以下の説明では、これらを簡略化して使用権情報と呼ぶことにする。

【０２６１】ユーザがシステムで使用する重要な情報（ここでは、コンテンツの使用権）を入手する際は、予めユーザ側２００毎に担当割当がなされている課金情報管理機関３２０に対し、ユーザ側２００からアクセスがなされる。上記ユーザ側２００から送られてくるコンテンツ使用権情報の入手要求のアクセスに対しては、課金情報管理機関３２０の使用権発行機能ブロック３６２が対応し、以下の手順に従って使用権の発行が行われる。

【０２６２】先ず、ユーザ側２００からは、購入依頼書送付Ｔ５１のように、使用権を購入したい旨の情報が課金情報管理機関３２０に対して送付される。使用権を購入したい旨の情報は、ユーザ側２００によって所定のフォーマットに従った購入依頼書の情報である。このようにネットワークを介し、この課金情報管理機関３２０の通信機能ブロック３６１に入力された上記購入依頼書の情報は、使用権発行機能ブロック３６２に送られる。

【０２６３】当該使用権発行機能ブロック３６２では、上記購入依頼書の情報を受け取ると、データベース機能ブロック３６７に保存されたユーザ情報を元にして、新しい使用権の情報を生成し、新規使用権送付Ｔ５２のように、当該使用権の情報をユーザ側２００に対して送付する。

【０２６４】ユーザ側２００は、上記新規使用権の情報の受取を確認すると、所定のフォーマットに従った受取確認書を作成し、受取確認書送付Ｔ５３のように、課金情報管理機関３２０の使用権発行機能ブロック３６２に送付する。

【０２６５】以上により、使用権の購入時の主な流れが終了する。なお、この図３２に挙げられている他の構成についての説明は後述する。

【０２６６】次に、図３３を用いて、コンテンツとコンテンツ鑑賞用の情報（ここでは使用条件とコンテンツ鍵）の流通の際の流れの主要部を説明する。

【０２６７】先ず、コンテンツ展示配信機関３１０のコンテンツ入手機能ブロック３４２は、コンテンツ請求書送付Ｔ６２のように、システム管理機関３３０に対して、ディジタルコンテンツを請求する。

【０２６８】当該コンテンツ請求書を受け取ったシステム管理機関３３０は、コンテンツ配布機能ブロック４０４において、要求されたコンテンツを流通できるように加工する。すなわち、このコンテンツ配布機能ブロック４０４では、ユーザ側２００に送付可能な状態のディジタルコンテンツ（暗号化されたディジタルコンテンツ）を生成する。この加工されたディジタルコンテンツは、コンテンツ送付６３のように、コンテンツ展示配信機関３１０に送られる。

【０２６９】当該コンテンツ展示配信機関３１０では、上記加工されたディジタルコンテンツを、コンテンツデータベース機能ブロック３４５に保存する。

【０２７０】また、システム管理機関３３０のコンテンツ配布機能ブロック４０４では、コンテンツ鑑賞用の情報として、コンテンツＩＤと使用条件と暗号化されたコンテンツを復号するためのコンテンツ鍵とを、コンテンツ鑑賞用情報送付Ｔ６４のように、課金情報管理機関３２０に送付する。

【０２７１】課金情報管理機関３２０では、上記コンテンツ鑑賞用の情報を、コンテンツ鍵・使用条件受取機能ブロック３６３にて受理し、データベース機能ブロック３６７に保存する。

【０２７２】次に、ユーザ側２００は、コンテンツ入手依頼Ｔ６１のように、コンテンツ展示配信機関３１０に対してアクセスし、コンテンツを入手する。すなわち、コンテンツ展示配信機関３１０は、通信機能ブロック３４１を介して上記ユーザ側２００からコンテンツの入手の要求がなされると、コンテンツデータベース機能ブロック３５４に保存している暗号化されたディジタルコンテンツを読み出し、当該読み出したディジタルコンテンツをユーザ側２００の送付する。

【０２７３】その後、ユーザ側２００は、コンテンツ鑑賞用情報請求Ｔ６５にて課金情報管理機関３２０に対してアクセスし、コンテンツ鑑賞用情報送付Ｔ６６のようにコンテンツ鑑賞用の情報を入手する。すなわち、課金情報管理機関３２０では、通信機能ブロック３６１を介して、上記ユーザ側２００からコンテンツ鑑賞用の情報として使用条件とコンテンツ鍵の請求がなされると、コンテンツ鍵・使用条件発行機能ブロック３６４からコンテンツ鍵と使用条件とを発行し、これらを通信機能ブロック３６１を介してユーザ側２００に送付する。

【０２７４】以上により、コンテンツとコンテンツ鑑賞用の情報の流通の際の流れが終了する。なお、この図３３に挙げられている他の構成についての説明は後述する。

【０２７５】次に、図３４を用いて、コンテンツが実際に鑑賞されたときの精算、すなわちコンテンツ使用料金の精算の流れの主要部を説明する。

【０２７６】先ず、ユーザ側２００にてコンテンツの鑑賞が行われた後、当該ユーザ側２００からは、精算書送付Ｔ７１のように、例えば前述のようにしてポイント使用情報すなわちコンテンツの使用記録が課金情報管理機

関３２０に対して送付される。このように通信機能ブロック３６１を介して上記ユーザ側２００から上記コンテンツ使用記録の送付を受けると、課金情報管理機関３２０の精算手続き受付機能ブロック３６５にて当該コンテンツ使用記録を受け取り、これに対応する精算確認書を発行する。当該精算確認書は、精算確認書送付Ｔ７３のように、同じく通信機能ブロック３６１を介してユーザ側２００に送付される。これにより、ユーザ側２００は精算が行われたことを知ることができる。

【０２７７】次に、課金情報管理機関３２０の精算手続き受付機能ブロック３６５は、使用権発行機能ブロック３６２から使用権発行情報を発行させる。この使用権発行情報は、上記ユーザ側２００から送られてきたコンテンツ使用記録と共に、通信機能ブロック３６１を介し、ユーザ決済・コンテンツ使用記録送付Ｔ７４としてシステム管理機関３３０に送付される。

【０２７８】システム管理機関３３０は、集金及び分配機能ブロック４０５にて、各地に分散している課金情報管理機関３２０から送付されてきた情報をまとめ、集金額と集金先と お金の分配先を集計し、実際の金融機関を通して決済する。

【０２７９】以上により、コンテンツ使用料金の精算の流れが終了する。なお、この図３４に挙げられている他の構成についての説明は後述する。

【０２８０】上述の図３０から図３４までの説明において、コンテンツ展示配信機関３１０、課金情報管理機関３２０、システム管理機関３３０とユーザ側２００との間のデータ送受や、コンテンツ展示配信機関３１０、課金情報管理機関３２０とシステム管理機関３３０との間のデータ送受においても、前述同様にデータの暗号化と復号化が行われていることは言うまでもない。またこの暗号化と復号化においても、公開鍵暗号方式と共通鍵暗号方式の何れを用いても良いし、前述したようにコンテンツ鍵や共通鍵の暗号化方式としては公開鍵暗号方式を使用し、メッセージや各種の書類等の暗号化方式としては共通鍵暗号方式を使用することができる。また、これら暗号化と共に前記乱数を用いたセキュリティ向上の手法や、コンテンツを扱う際の暗号化と圧縮の処理単位の最小公倍数化を使用することも可能である。

【０２８１】次に、上述した各機関３１０、３２０、３３０の具体的な構成について簡単に説明する。

【０２８２】先ず、図３５を用いてコンテンツ展示配信機関３１０の構成の説明を行う。

【０２８３】この図３５において、当該コンテンツ展示配信機関３１０は、大別して、ユーザ側２００とシステム管理機関３３０との間の通信機能を担当する通信機能ブロック３４１と、コンテンツの入手機能を担当するコンテンツ入手機能ブロック３４２と、コンテンツの展示機能を担当するコンテンツ展示機能ブロック３４３と、精算を担当する精算機能ブロック３４４と、コンテンツを保存するコンテンツデータベース機能ブロック３４５とからなる。

【０２８４】上記コンテンツ入手機能ブロック３４２は、システム管理機関３３０に対してコンテンツを請求するときの請求書の作成を担当するコンテンツ請求書作成機能部３５１と、システム管理機関３３０からコンテンツを受け取ったときの受領書の作成を担当するコンテンツ受領書作成機能部３５２と、これらあつかったコンテンツとコンテンツデータベース機能ブロック３４５に保存しているコンテンツとの対応を担当するコンテンツデータベース対応機能部３５３とからなる。

【０２８５】上記コンテンツ展示機能ブロック３４３は、実際に仮想店舗にコンテンツを展示する機能を担当するコンテンツ展示機能部３５４と、これら展示しているコンテンツと上記コンテンツデータベース機能ブロック３４５に保存しているコンテンツとの対応を担当するコンテンツデータベース対応機能部３５５とからなる。

【０２８６】上記精算機能ブロック３４４は、領収書を発行する機能を担当する領収書発行機能部３５６と、金融機関２２０との間の対応を担当する金融機関対応機能部３５７とからなる。

【０２８７】次に、図３６を用いて、課金情報管理機関３２０の構成の説明を行う。

【０２８８】この図３６において、当該課金情報管理機関３２０は、大別して、ユーザ側２００とシステム管理機関３３０との間の通信機能を担当する通信機能ブロック３６１と、使用権を発行する機能を担当する使用権発行機能ブロック３６２と、コンテンツ鍵と使用条件の受け取りを担当するコンテンツ鍵・使用条件受取機能ブロック３６３と、コンテンツ鍵と使用条件の発行を担当するコンテンツ鍵・使用条件発行機能ブロック３６４と、精算手続きの受け付け機能を担当する精算手続き受付機能ブロック３６５と、分配と受け取りの機能を担当する分配受取機能ブロック３６６と、データベース機能ブロック３７６とからなる。

【０２８９】上記使用権発行機能ブロック３６２は、購入依頼書の確認機能を担当する購入依頼書確認機能部３７１と、クライアントすなわちユーザ側２００の使用権の残高（ポイント情報の残高）や使用記録（ポイント使用情報）等のデータの確認を担当するポイントデータ確認機能部３７２と、使用権を発生する機能を担当する使用権発生機能部３７３と、使用権の送付書を作成する機能を担当する使用権送付書作成機能部３７４と、使用権と使用権送付書を実際に送付する機能を担当する送付機能部３７５と、使用権の受け取り書の確認を担当する使用権受取確認機能部３７６と、発行した使用権の情報を保存する機能を担当する使用権発行情報保存機能部３７７とからなる。

【０２９０】上記コンテンツ鍵・使用条件受取機能ブロック３６３は、コンテンツ鍵と使用条件の受取を担当す

る受取機能部３７８と、コンテンツ鍵と使用条件を保存する保存機能部３７９とからなる。

【０２９１】上記コンテンツ鍵・使用条件発行機能ブロック３６４は、コンテンツ鍵と使用条件の入手依頼を受信する機能を担当する受信機能部３８０と、コンテンツ鍵と使用条件をデータベース機能ブロック３６７から検索して探し出す機能を担当する検索機能部３８１と、コンテンツ鍵と使用条件を暗号化して送付する機能を担当する送信機能部３８２と、コンテンツ鍵と使用条件の受取書の確認機能を担当する確認機能部３８３とからなる。

【０２９２】上記精算手続き受付機能ブロック３６５は、暗号化されているコンテンツ使用記録（ポイント使用情報）を受信して復号化する機能を担当するコンテンツ使用記録受信機能部３８４と、コンテンツ使用記録の確認を担当するコンテンツ使用記録確認機能部３８５と、コンテンツ使用記録をデータベース機能ブロック３６７の保存する機能を担当するコンテンツ使用記録保存機能部３８６と、精算手続きの完了書を作成する機能を担当する完了書作成機能部３８７と、コンテンツ使用記録をまとめて編集する機能を担当するまとめ機能部３８９とからなる。

【０２９３】上記分配受取機能ブロック３６６は、集金を行う際の資料を請求する資料請求書の確認機能を担当する請求書確認機能部３９０と、システム管理機関３３０に対して提出するコンテンツ使用記録の報告書を作成する機能を担当する使用記録報告書作成機能部３９１と、システム管理機関３３０に対して提出する使用権発行情報の報告書を作成する機能を担当する使用権発行報告書作成機能部３９２と、報告書の受信確認書の確認機能を担当する確認書確認機能部３９３とからなる。

【０２９４】データベース機能ブロック３６７は、使用権のデータを保存する機能を担当する使用権データベース機能部３９４と、コンテンツ鍵と使用条件のデータを保存する機能を担当するコンテンツ鍵・使用権データベース機能部３９５と、コンテンツ使用記録を保存するコンテンツ使用記録データベース機能部３９６と、ユーザに関する情報を保存するユーザ管理データベース機能部３９７とからなる。

【０２９５】次に、図３７を用いて、システム管理機関３３０の構成の説明を行う。

【０２９６】この図３７において、当該システム管理機関３３０は、大別して、ユーザ側２００、コンテンツ展示配信機関３１０、及び課金情報管理機関３２０との間の通信機能を担当する通信機能ブロック４０１と、ユーザ加入の際のサポートを行うユーザ加入サポート機能ブロック４０２と、コンテンツの配布を担当するコンテンツ配布機能ブロック４０４と、データベース機能ブロック４０３と、集金と分配の機能を担当する集金及び分配機能ブロック４０５とからなる。

【０２９７】上記ユーザ加入サポート機能ブロック４０２は、加入申請書の作成と送信を担当する加入申請書作成送信機能部４１１と、暗号化された共通鍵を受信して復号化する機能を担当する共通鍵受信機能部４１２と、ユーザ側２００から送信されてきた加入申請書の確認機能を担当する加入申請書確認機能部４１３と、クライアントＩＤすなわちユーザＩＤを発生する機能を担当するＩＤ発生機能部４１４と、加入申請書をデータベース機能ブロック４０３に保存する機能を担当する加入申請書保存機能部４１５と、クライアント機能を生成するクライアント機能生成機能部４１６と、登録情報をデータベース機能ブロック４０３に保存する機能を担当する登録情報保存機能部４１７とからなる。

【０２９８】データベース機能ブロック４０３は、ユーザの情報を保存管理するユーザ管理データベース機能部４１８と、コンテンツを保存するコンテンツデータベース機能部４１９と、課金情報管理機関３２０の情報を保存管理する課金情報管理機関データベース機能部４２０と、コンテンツ展示配信機関３１０の情報を保存管理するコンテンツ展示配信機関データベース機能部４２１とからなる。

【０２９９】コンテンツ配信機能ブロック４０４は、コンテンツの請求書の確認機能を担当する請求書確認機能部４２２と、生コンテンツすなわち加工前のコンテンツ（ソースデータ）をデータベース機能ブロック４０３のコンテンツデータベース機能部４１９から検索する機能を担当するコンテンツ検索機能部４２３と、コンテンツＩＤを生成するコンテンツＩＤ生成機能部４２４と、コンテンツ鍵を生成するコンテンツ鍵生成機能部４２５と、コンテンツ使用条件を生成するコンテンツ使用条件生成機能部４２６と、生コンテンツすなわち加工前のコンテンツを圧縮するコンテンツ圧縮機能部４２７と、コンテンツの暗号化を行うコンテンツ加工機能部４２８と、コンテンツＩＤとコンテンツ鍵と使用条件とをデータベース機能ブロック４０３のコンテンツデータベース機能部４１９に保存する機能を担当する保存機能部４２９と、コンテンツを通信機能ブロック４０１を介して送付する機能を担当するコンテンツ送付機能部４３０と、コンテンツの受領書を確認する機能を担当するコンテンツ受領書確認機能部４３１と、コンテンツＩＤとコンテンツ鍵と使用条件を通信機能ブロック４０１を介して送付する機能を担当するＩＤ・鍵・使用条件送付機能部４３２と、コンテンツＩＤとコンテンツ鍵と使用条件の受領書を確認する機能を担当するＩＤ・鍵・使用条件受領書確認機能部４３３とからなる。

【０３００】集金及び分配機能ブロック４０５は、集金に使用する資料の請求書を作成する資料請求書作成機能部４３４と、コンテンツ使用権を通信機能ブロック４０１を介して受信する機能を担当するコンテンツ使用権受信機能部４３５と、コンテンツ使用記録を通信機能ブロ

ック４０１を介して受信する機能を担当するコンテンツ使用記録受信機能部４３６と、受信の確認書を作成する機能を担当する受信確認書作成機能部４３７と、ユーザへ請求する請求額の計算と請求書の作成を行う請求書の作成を行う計算・請求書作成機能部４３８と、使用により集金した使用金を権利者に分配する際の分配金の計算と納付書の作成を行う計算・納付書作成機能部４３９とからなる。

【０３０１】次に、当該他の実施の形態のシステムに対応するユーザ側２００の構成を、図３８を用いて説明する。なお、この図３８は、前記プレーヤ１とユーザ端末５０の各機能をまとめて表している。

【０３０２】この図３８において、当該ユーザ側２００の構成は、大別すると、システム管理機関３３０、コンテンツ展示配信機関３１０、及び課金情報管理機関３２０との間の通信機能を担当する通信機能ブロック４５１と、コンテンツの入手を担当するコンテンツ入手機能ブロック４５２と、ポイント情報やコンテンツ鍵、使用条件等の使用権の購入を担当する使用権購入機能ブロック４５３と、コンテンツ鍵と使用条件の入手を担当するコンテンツ鍵・使用条件入手機能ブロック４５４と、精算手続きを担当する精算手続き機能ブロック４５５と、システムへの加入をサポートする機能を担当するユーザ加入サポート機能ブロック４５６と、コンテンツの鑑賞と課金の機能を担当するコンテンツ鑑賞課金機能ブロック４５７と、データベース機能ブロック４５８とからなる。

【０３０３】上記コンテンツ入手機能ブロック４５２は、実際にコンテンツを入手する機能を担当するコンテンツ入手機能部４６１と、コンテンツを記憶メディアに保存させる機能を担当するコンテンツ保存機能部４６２とからなる。

【０３０４】使用権購入機能ブロック４５３は、使用権の購入依頼書を作成する購入依頼書作成機能部４６３と、クライアント（ユーザ）の使用権の残高（ポイント残高）や使用記録（ポイント使用情報）等のデータのまとめを担当するまとめ機能部４６４と、使用権としての各情報をインストールする機能を担当する使用権インストール機能部４６５と、使用権受取書を作成する使用権受取書作成機能部４６７とからなる。

【０３０５】コンテンツ鍵・使用条件入手機能ブロック４５４は、コンテンツ鍵と使用条件の入手依頼書を作成する入手依頼書作成機能部４６８と、コンテンツ鍵と使用条件の受信を担当する受信機能部４６９と、コンテンツ鍵と使用条件の受取書を作成する受取書作成機能部４７０とからなる。

【０３０６】精算手続き機能ブロック４５５は、コンテンツ使用記録（ポイント使用情報）のまとめを行うまとめ機能部４７１と、精算手続きの完了書の受信を担当する完了書受信機能部４７２とからなる。

【０３０７】上記ユーザ加入サポート機能ブロック４５６は、加入申請書の作成を担当する加入申請書作成機能部４７３と、クライアント機能のインストールサポートやユーザのプレーヤ１の初期化を担当するクライアント機能インストール機能部４７４、登録情報を作成する機能を担当する登録情報作成機能部４７５とからなる。

【０３０８】コンテンツ鑑賞課金機能ブロック４５７は、記憶メディアに保存されたコンテンツの検索を担当するコンテンツ検索機能部４７６と、使用権の確認を担当する使用権確認機能部４７７と、例えばコンテンツの選択を行うときに簡易的にコンテンツを再生する簡易コンテンツ鑑賞機能部４７８と、課金情報（ポイント情報）の管理を行う課金機能部４７９と、暗号化されているコンテンツを復号化するコンテンツ復号機能部４８０と、圧縮されているコンテンツを伸長するコンテンツ伸長機能部４８１と、例えば記憶メディアに保存されているコンテンツの内容を認識可能にするためのコンテンツビューア機能部４８２とからなる。

【０３０９】データベース機能ブロック４５８は、使用権のデータを保存する使用権データベース機能部４８３と、コンテンツ鍵と使用条件を保存するコンテンツ鍵・使用条件データベース機能部４８４と、コンテンツ使用記録を保存するコンテンツ使用記録データベース機能部４８５と、ユーザ情報を保存するユーザ情報データベース機能部４８６とからなる。

【０３１０】次に、上述したような各実施の形態のプレーヤ１とユーザ端末５０の具体的な使用形態について、図３９と図４０を用いて説明する。

【０３１１】図３９に示すように、プレーヤ１は、前記アナログ出力端子２とＰＣ用インターフェース端子３と記憶メディア用Ｉ／Ｏ端子４がプレーヤ１の筐体外に突き出た状態で配置されており、上記記憶メディア用Ｉ／Ｏ端子４には、記憶メディア６１が接続されるようになっている。また、これらプレーヤ１と記憶メディア６１は、例えばケース６０内に収納可能に形成されており、このケース６０の例えば一端側に上記プレーヤ１のアナログ出力端子２とＰＣ用インターフェース端子３が配置されるようになされている。

【０３１２】このプレーヤ１及び記憶メディア６１が収納されたケース６０は、上記プレーヤ１のアナログ出力端子２とＰＣ用インターフェース端子３が配置される側から、上記ユーザ端末５０としてのパーソナルコンピュータ５０の入出力ポート５３に挿入接続可能なように形成されている。

【０３１３】当該パーソナルコンピュータ５０は、コンピュータ本体に、ディスプレイ装置５２とキーボード５４とマウス５５とを備えた一般的な構成を有するものであるが、上記入出力ポート５３内には上記プレーヤ１のアナログ出力端子２及びＰＣ用インターフェース端子３と対応したインターフェースが形成されている。したが

って、上記プレーヤ１及び記憶メディア６１が収納されたケース６０を上記パーソナルコンピュータ５０の入出力ポート５３に挿入するだけで、上記プレーヤ１のアナログ出力端子２とＰＣ用インターフェース端子３が上記パーソナルコンピュータ５０と接続されるようになる。

【０３１４】上記図３９の例では、パーソナルコンピュータ５０の入出力ポート５３内に、上記プレーヤ１のアナログ出力端子２及びＰＣ用インターフェース端子３と対応したインターフェースを形成するようにしているが、例えば図４０に示すように、パーソナルコンピュータ５０の汎用入出力ポートのインターフェースに対応できるアダプタ６２を、上記プレーヤ１のアナログ出力端子２及びＰＣ用インターフェース端子３の間に配置することも可能である。

【０３１５】以上述べてきたことから、本発明の実施の形態のシステムにおいては、ディジタルコンテンツはシステムの共通鍵であるコンテンツ鍵にて暗号化されているので、本実施の形態のシステムに登録したユーザ（プレーヤ１）であれば、この暗号化されたコンテンツを自由にコピーでき、コンテンツ鍵を入手しさえすればこのコンテンツの鑑賞も可能である。したがって、このコンテンツ（暗号化されたコンテンツの）記憶メディアへのインストールも簡単に行える。一方、本実施の形態システムに準拠していない端末装置では、暗号化されたディジタルコンテンツを復号できないので、コンテンツの著作権や当該コンテンツの権利者の権利は保護される。

【０３１６】また、本発明の実施の形態システムによれば、ポイント情報をプリペイド方式（料金前払い方式）により補充することにし、コンテンツ鑑賞時にポイント情報が減額されるようにするとともに、そのポイントの使用情報を収集するようにしているので、使用済みのポイントに関する権利をもつ権利者（著作権者等）及びコンテンツ販売店舗等は、鑑賞代金の回収が可能である。

【０３１７】さらに、ポイント情報やポイント使用情報のデータのやりとりの際には、前述したように暗号化が施されているので、セキュリティ性が向上している。例えば全く前回のデータと同じものを偽造して課金用のポイント情報を盗もうとしても、前述したように、システム側とプレーヤ側とで連動した乱数（セキュリティＩＤ）を使用し、両者が一致していることを確認してから取引を行うものとしているので、安全である。

【０３１８】またさらに、プレーヤの主要構成要素は１チップ化されており、鍵情報や復号化されたディジタルコンテンツを外部に取り出すことが困難となっている。このプレーヤ１は、当該プレーヤ１の破壊によるデータ横取りを防ぐためにプレーヤ１自体にタンパーレジスタンス機能を備えている。

【０３１９】上述したように、本発明の実施の形態によれば、セキュリティ上強度の高いディジタルコンテンツ配信システムが構築されている。

【０３２０】なお、上述のディジタルコンテンツとしては、ディジタルオーディオデータの他に、ディジタルビデオデータ等の各種のものを挙げることができる。上記ディジタルビデオデータとして動画像データ（オーディオデータも含む）使用した場合、前記圧縮の手法としては、例えばＭＰＥＧ（Moving Picture Image CodingExperts Group）等の圧縮手法を使用できる。なお、上記ＭＰＥＧは、ＩＳＯ（国際標準化機構）とＩＥＣ（国際電気標準会議）のＪＴＣ（Joint Technical Committee）１のＳＣ（Sub Committee）２９のＷＧ（Working Group）１１において まとめられた動画像符号化方式の通称であり、ＭＰＥＧ１，ＭＰＥＧ２，ＭＰＥＧ４等がある。

【０３２１】さらに、上記暗号化の手法としては、前述したように、例えばいわゆるＤＥＳ（Data Encryption Standard）と呼ばれている暗号化手法を使用することができる。なお、ＤＥＳとは、米国のＮＩＳＴ（National Institute of Standards and Technology）が１９７６年に発表した標準暗号方式（暗号アルゴリズム）である。具体的には、６４ビットのデータブロック毎にデータ変換を行うものであり、関数を使った変換を１６回繰り返す。上記ディジタルコンテンツやポイント情報等は、当該ＤＥＳを用い、いわゆる共通鍵方式にて暗号化されている。なお、上記共通鍵方式とは、暗号化するための鍵データ（暗号鍵データ）と復号化するための鍵（復号鍵データ）が同一となる方式である。

【０３２２】また、前記図１のプレーヤ１の共通鍵保管メモリ２２や通信用鍵保管メモリ２１、ポイント使用情報格納メモリ２９、ポイント情報格納メモリ２８等には、例えばいわゆるＥＥＰＲＯＭ（電気的に消去可能なＲＯＭ）を使用できる。

【０３２３】他に記憶メディアとしては、例えばハードディスクやフロッピィディスク、光磁気ディスク，相変化型光ディスク等の記録媒体、或いは半導体メモリ（ＩＣカード等）の記憶メディアを使用できる。

【０３２４】その他、上述の実施の形態では、コンテンツの選択や仮想店舗２３０に展示されたコンテンツの内容確認等の際には、ユーザ端末５０のキーボード５４やマウス５５、ディスプレイ装置５２を使用して選択、確認等を行っていたが、これらキーボードやマウス、ディスプレイ装置に機能を簡略化して、プレーヤ１に持たせることも可能である。すなわち、図２０ように、入力キー部６や表示部７をプレーヤ１に設けることも可能である。

【０３２５】

【発明の効果】以上の説明で明らかなように、本発明によれば、簡単に持ち運びができて何時でも何処でもディジタルコンテンツを楽しむことが可能であり、また、ディジタルコンテンツのコピー或いは不当な使用への防御として十分運用に耐え、且つ経済的なシステムを構築す

ることをも可能である。

【図面の簡単な説明】

【図１】本発明の実施の形態のディジタルコンテンツ配布システムの全体構成を示すシステム構成図である。

【図２】本発明の実施の形態のシステムに対応するプレーヤの具体的構成を示すブロック回路図である。

【図３】本発明の実施の形態のシステムに対応する管理センタの具体的構成を示すブロック回路図である。

【図４】本実施の形態のシステムにおいてプレーヤの購入時の手順の説明に用いる図である。

【図５】本実施の形態のシステムにおいてディジタルコンテンツの検索からプレーヤ用の記憶メディアへのディジタルコンテンツのインストールまでの手順の説明に用いる図である。

【図６】実施の形態のシステムにおいて課金用のポイント情報の購入と当該ディジタルコンテンツを使用した場合の精算の手順の説明に用いる図である。

【図７】実施の形態のシステムにおいて課金代金の分配の手順の説明に用いる図である。

【図８】実施の形態のシステムにおいてポイント購入時のプレーヤにおける処理の流れを示すフローチャートである。

【図９】実施の形態のシステムにおいてポイント購入時のユーザ端末における処理の流れを示すフローチャートである。

【図１０】実施の形態のシステムにおいてポイント購入時の管理センタにおける処理の流れを示すフローチャートである。

【図１１】実施の形態のシステムにおいてポイント購入時の情報送受のシーケンスを示す図である。

【図１２】実施の形態のシステムにおいてディジタルコンテンツの入手時のプレーヤにおける処理の流れを示すフローチャートである。

【図１３】実施の形態のシステムにおいてディジタルコンテンツの入手時のユーザ端末における処理の流れを示すフローチャートである。

【図１４】実施の形態のシステムにおいてディジタルコンテンツの入手時の管理センタにおける処理の流れを示すフローチャートである。

【図１５】実施の形態のシステムにおいてディジタルコンテンツの入手時の情報送受のシーケンスを示す図である。

【図１６】実施の形態のシステムにおいてコンテンツ鍵及び使用条件の入手時のプレーヤにおける処理の流れを示すフローチャートである。

【図１７】実施の形態のシステムにおいてコンテンツ鍵及び使用条件の入手時のユーザ端末における処理の流れを示すフローチャートである。

【図１８】実施の形態のシステムにおいてコンテンツ鍵及び使用条件の入手時の管理センタにおける処理の流れを示すフローチャートである。

【図１９】実施の形態のシステムにおいてコンテンツ鍵及び使用条件の入手時の情報送受のシーケンスを示す図である。

【図２０】実施の形態のシステムにおいてプレーヤとユーザ端末を用いてディジタルコンテンツを実際に鑑賞する際の処理の流れを示すフローチャートである。

【図２１】実施の形態のシステムにおいてポイント使用情報返却時のプレーヤにおける処理の流れを示すフローチャートである。

【図２２】実施の形態のシステムにおいてポイント使用情報返却時のユーザ端末における処理の流れを示すフローチャートである。

【図２３】実施の形態のシステムにおいてポイント使用情報返却時の管理センタにおける処理の流れを示すフローチャートである。

【図２４】実施の形態のシステムにおいてポイント使用情報返却時の情報送受のシーケンスを示す図である。

【図２５】暗号化と圧縮の処理単位の最小公倍数にて復号化と伸長を行う際の処理の流れを示すフローチャートである。

【図２６】暗号化と圧縮の処理単位の最小公倍数の単位毎の復号化及び伸長処理を行う構成を示すブロック回路図である。

【図２７】セキュリティＩＤとしての乱数を発生する具体的構成を示すブロック回路図である。

【図２８】共通鍵を公開鍵暗号方式にて暗号化して送信する際に乱数が挿入される様子を説明するための図である。

【図２９】受信文から乱数が取り出されて正当性の確認がなされる様子を説明するための図である。

【図３０】システム側の機能を分割したときの各機関の説明に用いる図である。

【図３１】システム側の機能を分割した実施の形態において、ユーザのシステムへの加入時の流れの主要部を説明するための図である。

【図３２】システム側の機能を分割した実施の形態において、ポイント情報の購入や暗号化されたディジタルコンテンツの復号用の鍵等の入手時の情報の流れの主要部を説明するための図である。

【図３３】システム側の機能を分割した実施の形態において、コンテンツとコンテンツ鑑賞用の情報の流通の際の流れの主要部を説明するための図である。

【図３４】システム側の機能を分割した実施の形態において、コンテンツが実際に鑑賞されたときの精算の流れの主要部を説明するための図である。

【図３５】システム側の機能を分割した実施の形態において、コンテンツ展示配信機関の構成を示すブロック図である。

【図３６】システム側の機能を分割した実施の形態にお

いて、課金情報管理機関の構成を示すブロック図である。

【図３７】システム側の機能を分割した実施の形態において、システム管理機関の構成を示すブロック図である。

【図３８】システム側の機能を分割した実施の形態において、ユーザ側の構成を示すブロック図である。

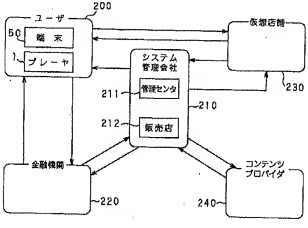
【図３９】プレーヤとユーザ端末の具体的な使用形態の一例の説明に用いる図である。

【図４０】プレーヤとユーザ端末の具体的な使用形態の他の例の説明に用いる図である。

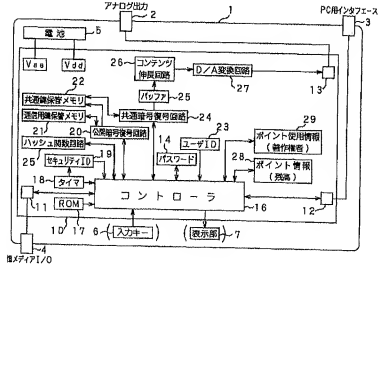
【符号の説明】

１　プレーヤ、　２　アナログ出力端子、　３　ＰＣ用＊インターフェース端子、　４　記憶メディア用Ｉ／Ｏ端子、　１６　コントローラ、　１９　セキュリティＩＤ発生回路、　２０　公開暗号復号回路、　２１　通信用鍵保管メモリ、２２　共通鍵保管メモリ、　２３　ユーザＩＤ格納メモリ、　２４　共通暗号復号回路、　２５　バッファメモリ、　２６　伸長回路、　２７　Ｄ／Ａ変換回路、　５０　ユーザ端末、　１００　コンテンツ管理機能ブロック、　１１０ユーザ管理機能ブロック、　１２０　使用情報管理機能ブロック、　１３０　管理機能ブロック、　２００　ユーザ側、　２１０　システム管理会社、　２１１管理センタ、　２２０　金融機関、　２３０…仮想店舗、　２４０　コンテンツプロバイダ

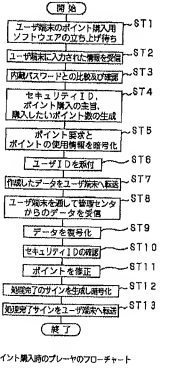
【図１】



【図２】

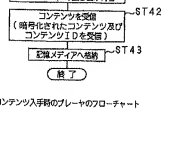


【図８】



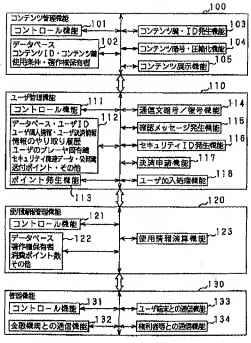
ポイント購入時のプレーヤのフローチャート

【図１２】

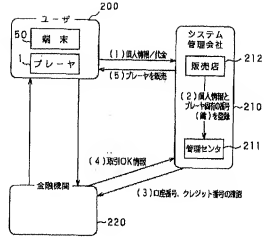


コンテンツ入手時のプレーヤのフローチャート

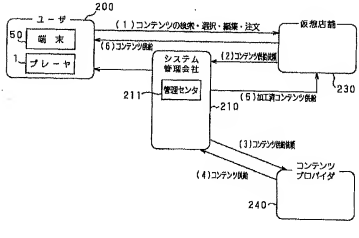
【図3】



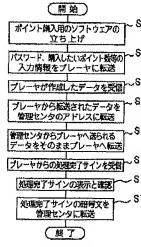
【図4】



【図5】

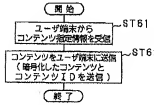


【図9】



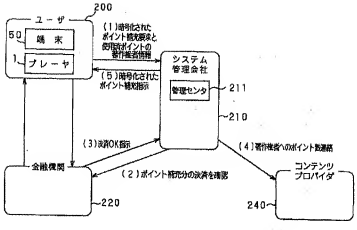
ポイント購入時のユーザ端末のフローチャート

【図14】

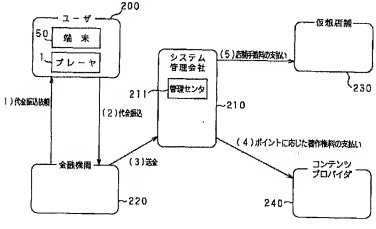


コンテンツ入手時の管理センタのフローチャート

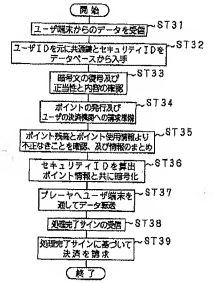
【図６】



【図７】

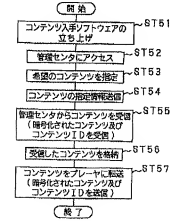


【図１０】



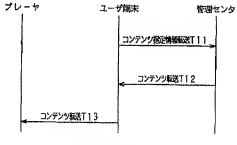
ポイント購入時の管理センタのフローチャート

【図１３】



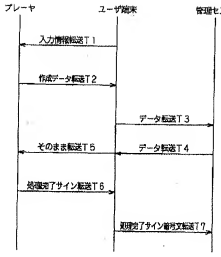
コンテンツ入手時のユーザ端末のフローチャート

【図１５】



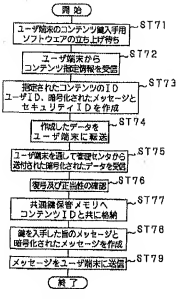
コンテンツ入手時のシーケンス

【図１１】



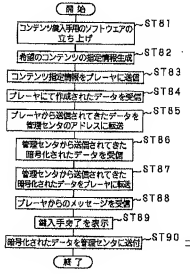
ポイント購入時のシーケンス

【図１６】



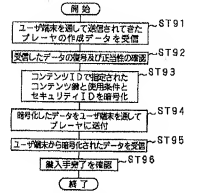
コンテンツ鍵・入手時のプレーヤのフローチャート

【図１７】



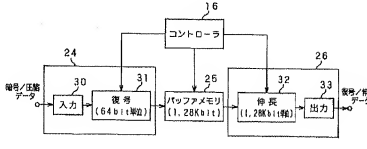
コンテンツ鍵・使用条件入手時のユーザ端末のフローチャート

【図１８】

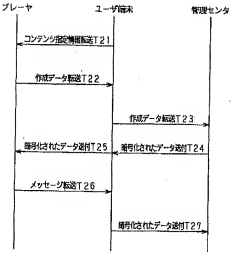


コンテンツ鍵・使用条件入手時の管理センタのフローチャート

【図２６】

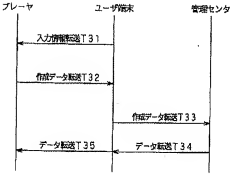


【図１９】



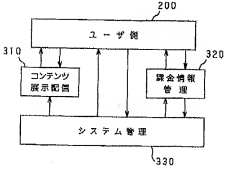
コンテンツ鍵・使用条件入手時のシーケンス

【図２４】

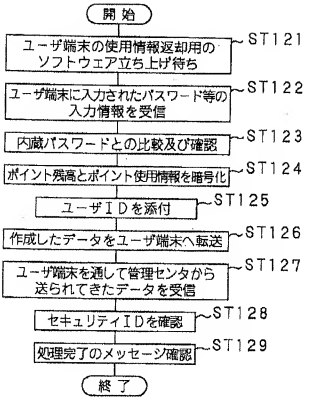


使用情報返却時のシーケンス

【図３０】

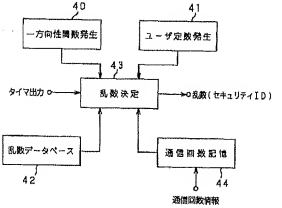


【図２１】

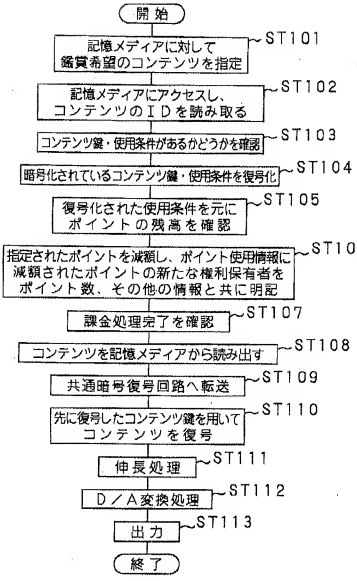


使用情報返却時のプレーヤのフローチャート

【図２７】

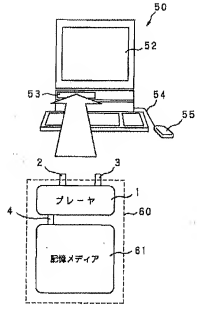


【図20】

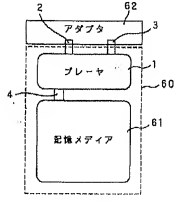


コンテンツ鑑賞時のプレーヤのフローチャート

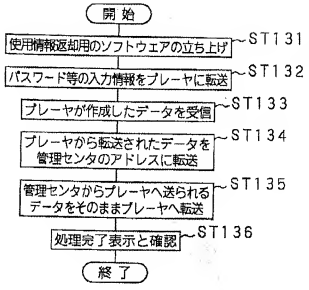
【図39】



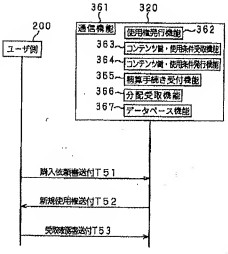
【図40】



【図２２】

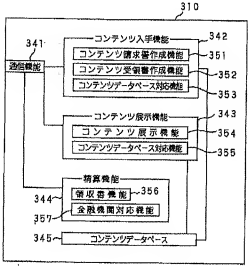


【図３２】

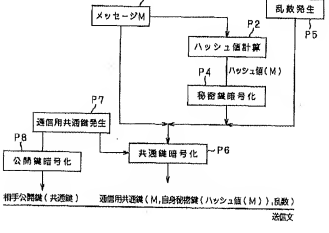


使用情報返却時のユーザ端末のフローチャート

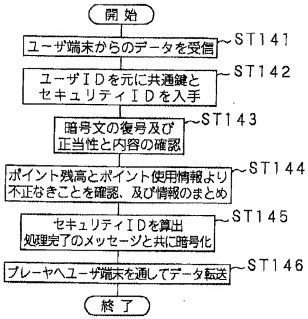
【図３５】



【図２８】

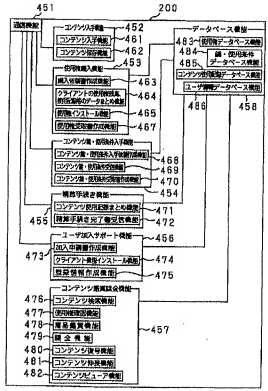


【図２３】

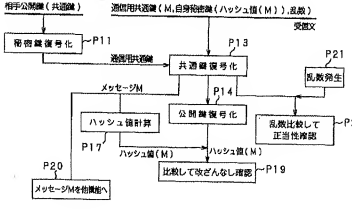


使用情報返却時の管理センタのフローチャート

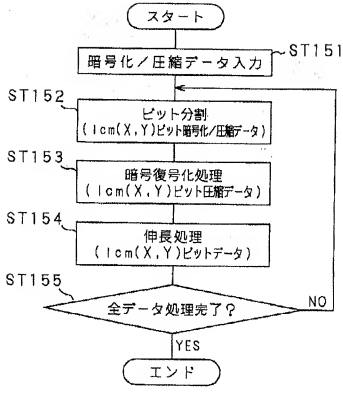
【図３８】



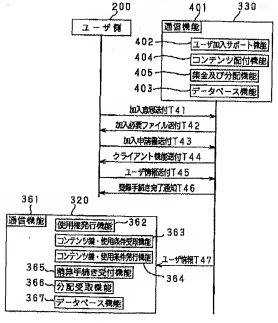
【図２９】



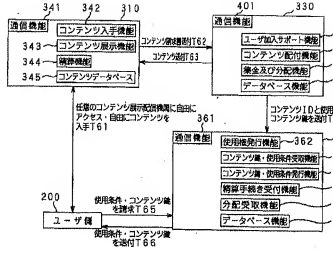
【図25】


スタート
暗号化／圧縮データ入力
ST151
ST152
ビット分割
（1cm(X,Y)ビット暗号化/圧縮データ）
ST153
暗号復号化処理
（1cm(X,Y)ビット圧縮データ）
ST154
伸長処理
（1cm(X,Y)ビットデータ）
ST155
全データ処理完了？
NO
YES
エンド

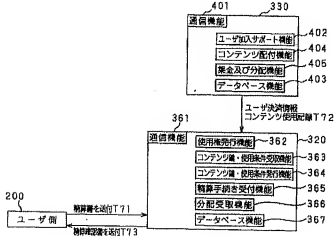
【図31】


200
401
330
ユーザ側
通信機能
402
ユーザ加入サポート機能
404
コンテンツ配付機能
405
課金及び分配機能
403
データベース機能
加入意思送付T41
加入必要ファイル送付T42
加入申請書送付T43
クライアント機能送付T44
ユーザ情報送付T45
登録手続き完了通知T46
361
320
通信機能
使用権発行機能
362
363
コンテンツ鍵・使用条件受取機能
コンテンツ鍵・使用条件発行機能
ユーザ情報T47
365
課金手続き受付機能
364
366
分配受取機能
367
データベース機能

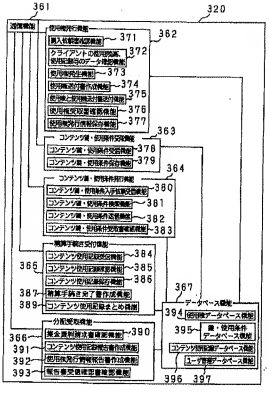
【図３３】


341
342
310
401
330
通信機能
コンテンツ入手機能
コンテンツ展示機能
343
344
345
課金機能
コンテンツデータベース
コンテンツ登録通知T62
コンテンツ送付T63
ユーザ加入サポート機能
コンテンツ配付機能
集金及び分配機能
データベース機能
402
404
405
403
任意のコンテンツ流行配信時期に自由にアクセス・自由にコンテンツを入手T61
コンテンツIDと使用条件・コンテンツ鍵を送付T64
361
通信機能
使用権発行機能
362
320
コンテンツ鍵・使用条件受取機能
363
コンテンツ鍵・使用条件発行機能
364
精算手続き受付機能
365
分配受取機能
366
データベース機能
367
200
ユーザ側
使用条件・コンテンツ鍵を請求T65
使用条件・コンテンツ鍵を送付T66

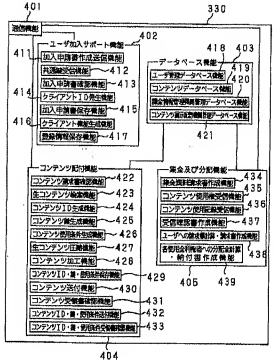
【図３４】


401
330
通信機能
ユーザ加入サポート機能
コンテンツ配付機能
集金及び分配機能
データベース機能
402
404
405
403
ユーザ決済情報コンテンツ使用記録T72
361
通信機能
使用権発行機能
362
320
コンテンツ鍵・使用条件受取機能
363
コンテンツ鍵・使用条件発行機能
364
精算手続き受付機能
365
分配受取機能
366
データベース機能
367
200
ユーザ側
精算書を送付T71
精算確認書を送付T73

【図３６】



【図３７】



フロントページの続き

(51)Int.Cl.[6]	識別記号	FI	
H04L 9/08		H04M 15/00	Z
12/14		G06F 15/21	Z
H04M 15/00		H04L 9/00	601E
			601A
		11/02	F